UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SÓCIOECONÔMICO
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO DE RELAÇÕES INTERNACIONAIS

Eduardo de Rê

Ciberespaço e Segurança Cibernética: as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil

Florianópolis
2021

Eduardo de Rê

Ciberespaço e Segurança Cibernética: **as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil**

Trabalho de Conclusão de Curso de Graduação em Relações Internacionais da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Relações Internacionais.
Orientadora: Prof.(a) Danielle Jacon Ayres Pinto, Dra.

Florianópolis

2021

Ficha de identificação

de Rê, Eduardo
Ciberespaço e Segurança Cibernética: as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil / Eduardo de Rê ; orientadora, Danielle Jacon Ayres Pinto, 2021.
108 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Sócio Econômico, Graduação em Relações Internacionais, Florianópolis, 2021.

Inclui referências.

1. Relações Internacionais. 2. Ciberespaço, Segurança Cibernética, Estratégia Nacional. I. Ayres Pinto, Danielle Jacon. II. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. III. Título.

Eduardo de Rê

Ciberespaço e Segurança Cibernética: **as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil**

Florianópolis, 10 de maio de 2021

O presente Trabalho de Conclusão de Curso foi avaliado e aprovado pela banca examinadora composta pelos seguintes membros:

Prof.(a) Graciela De Conti Pagliari, Dra.
Instituição: Universidade Federal de Santa Catarina

Prof. Gills Vilar Lopes, Dr.
Instituição: Universidade da Força Aérea

Certifico que esta é a **versão original e final** do Trabalho de Conclusão de Curso que foi julgado adequado para obtenção do título de Bacharel em Relações Internacionais por mim e pelos demais membros da banca examinadora.

ICP-Edu
Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 14/05/2021 12:10:06-0300
CPF: 291.367.488-70
Verifique as assinaturas em https://v.ufsc.br

Prof.(a) Danielle Jacon Ayres Pinto, Dra.
Orientadora

Florianópolis, 2021

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer à minha família, que me deu todo o suporte e as condições necessárias para que eu pudesse chegar até aqui. Em especial, agradeço aos meus pais, Dirceu e Elisandra, que sempre estiveram ao meu lado me apoiando e amparando emocionalmente, psicologicamente e materialmente. Muito obrigado por tudo.

Aos professores que tive durante a toda a minha vida e trajetória acadêmica, pessoas que dedicam suas vidas ao ensino e à educação, uma profissão nobre e essencial na formação de todo cidadão. Em especial agradeço à minha orientadora, professora Danielle Jacon Ayres Pinto, que me auxiliou não só na elaboração deste trabalho, mas em grande parte da minha graduação e vida acadêmica.

Aos meus amigos de vida e de UFSC que estiveram junto comigo durante esses anos. Suas companhias foram essenciais para minha evolução pessoal e profissional.

Por fim, mas não menos importante, agradeço ao sistema público de ensino e à UFSC, que proporcionam um caminho de luz e conhecimento para muitos brasileiros mesmo diante de muitos obstáculos.

RESUMO

O presente trabalho busca analisar de maneira comparativa as estratégias nacionais de segurança e defesa cibernética de Estados Unidos, China, Israel e Brasil. Buscando compreender as suas concepções e visões políticas sobre o espaço cibernético por meio, principalmente, dos documentos estratégicos oficiais publicados pelos governos dos respectivos países. A metodologia utilizada consiste em uma comparação qualitativa dos modelos cibernéticos dos países pesquisados a partir do método hipotético-dedutivo de que as estratégias das potências cibernéticas (EUA, China e Israel) possuem influência sobre o modelo cibernético de países periféricos como o Brasil. A pesquisa nasce devido ao intenso processo de digitalização das atividades humanas, especialmente em vista do rápido avanço de tecnologias de informação e comunicação. Essas tecnologias estão moldando a nossa vida e, consequentemente, afetando tanto as relações sociais quanto as relações internacionais. O espaço cibernético se tornou responsável por trazer novas possibilidades na realização de tarefas básicas e especializadas no cotidiano da vida humana, mas também fez com que novas ameaças que impactam diretamente a defesa e a segurança nacional emergissem. Com isso, o ciberespaço vem sendo reconhecido na política internacional como um novo domínio de poder, que diferente dos domínios tradicionais, tem por característica natural a ausência de fronteiras físicas, dificultando o seu controle e delimitação. Esse contexto somado ao fato de que o cenário internacional atual é marcado pela ausência de regulamentações e normas internacionais para o ciberespaço global, faz com que os Estados se vejam compelidos a tomar suas próprias medidas para lidar com ciberespaço, produzindo diretrizes e estratégias cibernéticas nacionais que coordenam e estruturam as ações que devem ser implementadas. Nesse sentido, os documentos governamentais são as principais fontes de análise para a compreensão de como esses países lidam com esse domínio. Sendo que eles indicam que há uma convergência entre os fatores considerados estratégicos pelos países analisados.

Palavras-chave: Ciberespaço, estratégia cibernética, segurança cibernética, defesa cibernética,

ABSTRACT

The present workpaper seeks to analyze, in a comparative way, the national cyber security and defense strategies of the United States, China, Israel and Brazil. Aiming to understand their conceptions and political views on cyberespace mainly through the official strategic documents published the governments of the respective countries. The methodoly used rely on a qualitative comparison of the cyber models of the countries surveyed, based on the hypothesis that the strategies of the cyber powers (U.S, China and Israel) have the influence on the cyber model of peripheral countries like Brazil. The research was born due to the intense process of digitalization of humans activities, especially because of the fast advance of information and communication technologies. These technologies are shaping our lives and, consequently, affecting both social and internacional relations. The cyberspace has become responsible for bringing new possibilities in the realization of basic and specialized tasks in the human daily life, but it has also produced new threats that directly impacts national defense and security. Therefore, the cyberspace has been reconized in international politics as a new domain of power, which unlike traditional domains, has the natural characteristic of the absence of physical borders, making it difficult to control and delimit. This context added to the fact that the current international scene is marked by the absence of international regulations and norms for the global cyberspace, makes States feel compelled to take their own measures to deal with cyberspace, formulating national cyber guidelines and strategies that coordinate and structure the actions that shall be executed. In this sense, government documents are the main sources of analysis to understand how theses countries deal with this new domain. Since 7hey indicate that there is a convergence between the factors considered strategic by the countries analyzed.

Keywords: Cyberspace, cyber strategy, cyber security, cyber defense

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA Advanced Research Projects Agency

CDCiber Centro de Defesa Cibernética

CERN Conselho Europeu para Pesquisa Nuclear

CERT Cyber Emergency Response Team

ComdCiber Comando de Defesa Cibernética

CT&I Ciência, Tecnologia e Inovação

DHS Department of Homeland State

DNS Sistema de Nomes e Domínio

DoD Department of Defense

END Estratégia Nacional de Defesa

ESG Escola Superior de Guerra

EUA Estados Unidos da América

FA Forças Armadas

GSI Gabinete de Segurança Institucional

HTML HyperText Markup Language

ICANN Internet Corporation for Assigned Names and Numbers

IDF Forças de Defesa de Israel

INCB Israel National Cyber Bureau

IP Protocolo da Internet

LGPD Lei Geral de Proteção de Dados

MD Ministério da Defesa

NCSA National Cyber Security Authority

NICE National Initiative for Cybersecurity Education

NIPP Plano Nacional de Proteção a Infraestrutura

NSFNET National Science Foundation Network

OCDE Organização para a Cooperação e Desenvolvimento Econômico

ONU Organização das Nações Unidas

OTAN Organização do Tratado do Atlântico Norte

P&D Pesquisa e Desenvolvimento

PND Plano Nacional de Defesa

PNUD Programa de Desenvolvimento das Nações Unidas

SCO Shanghai Cooperation Organization

SIC Segurança da Informação e Comunicação

SIGINT Inteligência de Sinais

SIMOC Simulador de Operações de Guerra Cibernética

SMDC Sistema Militar de Defesa Cibernética

TICs Tecnologias da Informação e Comunicação

UIT União Internacional de Telecomunicação

USCYBERCOM Comando Ciber dos Estados Unidos

WWW World Wide Web

SUMÁRIO

1 INTRODUÇÃO

A construção das sociedades em que vivemos perpassa pelas percepções dos seus riscos e ameaças, que acabam determinando pensamentos, ações e, por conseguinte, políticas, que acabam sendo estruturadas a partir do dimensionamento desses riscos. O espaço virtual não deixa de ser um novo aspecto para a sociedade contemporânea. Assim, a securitização desse ambiente se torna instrumental para a construção da realidade e para a constituição das percepções de riscos e ameaças em um nível global (RADU, 2014). Esse novo espaço, denominado de ciberespaço, está presente em quase todas as interações que temos hoje em dia, até mesmo geladeiras já possuem conexão à internet. As atividades humanas sofreram alterações graças a digitalização de tecnologias e o ciberespaço não apenas contribuiu na globalização dos negócios e mercados, mas também conectou pessoas e empresas, colaborando para a produção e consumo de informações em tempo real por todo o globo terrestre (KREMER; MULLER, 2014).

Contudo, essa modificação substancial que o espaço cibernético ocasionou trouxe novas ameaças juntamente com as facilitações. Com isso, discursos governamentais sobre os perigos e riscos cibernéticos começaram a ser cada vez mais presentes e relevantes no cenário internacional. A avaliação dos danos que o uso malicioso de tecnologias, em especial as tecnologias da informação e comunicação (TICs), pode causar para uma sociedade e para uma nação começaram a alertar os governos nacionais para a necessidade de securitizar esse novo espaço.

O fato de a sociedade moderna estar altamente dependente e interconectada com a digitalização da informação e da comunicação, intensificou a sua exposição a novas vulnerabilidades. Uma consequência direta desse fenômeno é o aumento da militarização do ciberespaço (MEHMETCIK, 2014). Isso ocorre devido a segurança desse novo espaço estar posicionada em uma linha de descendência de anteriores espaços de insegurança, que aparentemente foram convertidos em espaços seguros (BARNARD-WILLS; ASHENDEN, 2012). Nesse sentido, a militarização ocorre na tentativa de proteger as vulnerabilidades e criar controles em um espaço onde as incertezas e os riscos ainda não são mensuráveis.

O sentimento de insegurança das nações se mostrou válido principalmente após a ocorrência de grandes incidentes cibernéticos, como os ataques cibernéticos sofridos pela Estônia, em 2007, e o *Stuxnet*, em 2010, que chamaram a atenção de toda a comunidade internacional. O caso estoniano mostrou empiricamente como um país altamente dependente

de meios digitais e tecnologias da informação pode se encontrar em uma posição vulnerável. Isso porque já em 2007 a Estônia contava com o espaço cibernético para o funcionamento das suas infraestruturas, redes eletrônicas e serviços financeiros. Dessa forma, a desabilitação de servidores do parlamento e de capacidades cibernéticas do governo devido a ataques cibernéticos paralisaram a capacidade do Estado em reagir de modo efetivo (HERZOG, 2011). Já o ataque que ficou conhecido como *Stuxnet*, fez com que a frequência da corrente elétrica que gerava energia para as centrífugas nucleares no Irã fossem alteradas, causando alternâncias de velocidades e intervalos nas quais as máquinas não foram projetadas (FARWELL; ROHONZINSKI, 2011). Foi o primeiro incidente cibernético com consequências físicas.

Os eventos contribuíram para questionamentos sobre os potenciais efeitos de um ato hostil no ciberespaço, fazendo emergir interpretações sobre a ingerência do espaço cibernético em guerras e conflitos armados. Com isso, os Estados passaram a dar maior importância aos desafios que existem para governar e ter certo domínio sobre as ações efetuadas dentro do espaço virtual, especialmente em vista do cenário internacional atual, em que arquitetura da governança global do ciberespaço é marcada por múltiplas iniciativas, que buscam a cooperação e a redefinição dos papéis exercidos pelos atores (RADU, 2014), sem uma regulamentação central.

Nesse sentido, Barnard-Wills e Ashenden (2012) indicam que as características do ciberespaço são utilizadas na construção dos discursos políticos, como a ausência de governança, a capacidade de tornar todos vulneráveis e ser inevitavelmente ameaçador. Segundo os autores, essas características acabam servindo de justificativa para a securitização do espaço cibernético, com base no ato retórico de considerar determinado problema político como uma ameaça real e esta ser aceita. Dessa forma, muitos Estados tornaram públicas as suas compreensões e visões sobre o assunto, publicando diretrizes e estratégias nacionais para lidar com o espaço cibernético, estabelecendo objetivos e iniciativas que visam garantir a defesa e a segurança cibernética em seus respectivos países.

Esses documentos oficiais são hoje as fontes primárias existentes para entender a concepção dos Estados sobre esse novo domínio. Bem como para compreender as ações que eles pretendem tomar no âmbito interno e externo e como isso afeta as relações internacionais de um modo geral. Como já comentado, isso se deve ao estado anárquico em que o ciberespaço global se encontra hoje. Não há normas nem convenções internacionais específicas no âmbito da defesa cibernética, permitindo que os governos nacionais possam adotar os regulamentos e medidas que considerem necessários para a construção de um espaço virtual seguro (EILSTRUP-SANGIOVANNI, 2018).

Em vista disso, o presente trabalho busca como seu principal objetivo compreender as visões de Estados Unidos, China, Israel e Brasil perante o ciberespaço, por meio da análise dos seus principais documentos estratégicos de defesa e segurança cibernética. Possuindo os seguintes objetivos específicos: (i) compreender como a defesa e a segurança cibernética estão sendo tratadas na política internacional a partir dos países analisados; (ii) observar se há um certo padrão internacional na forma de abordar sobre o ciberespaço; (iii) observar se a estratégia cibernética brasileira se insere de maneira defasada no contexto internacional em comparação com as potências cibernéticas analisadas.

A natureza da pesquisa é exploratória e comparativa, em vista do objetivo de realizar um estudo comparado entre as visões, fatores e seguimentos estratégicos entre Israel, China, EUA e Brasil na área de defesa e segurança cibernética. Serão levados em consideração aspectos qualitativos dos modelos cibernéticos de cada país, por envolver questões que não se utilizam de dados numéricos e possuir um enfoque nas relações sociais e políticas entre Estados, organizações estatais e organizações não estatais.

A indagação de partida desta pesquisa é: Como o ciberespaço global não possui uma regulamentação internacional, os países periféricos acabam seguindo ou aderindo os modelos de estratégias cibernéticas de países avançados tecnologicamente e que possuem uma base institucional e legal para o ciberespaço já consolidada? Nesse sentido, a pergunta desperta a hipótese de que as estratégias nacionais de potências cibernéticas, como os EUA, China e Israel, promovem uma influência, ou um certo condicionamento, nas estratégias nacionais cibernéticas de países periféricos como o Brasil, que possui um baixo nível de digitalização tecnológica e uma estratégia cibernética nacional não totalmente estruturada. Nesse caso, as variáveis consideradas independentes são as estratégias nacionais de ciberdefesa e cibersegurança de Israel, Estados Unidos e China, enquanto que a variável dependente são as diretrizes e estratégias cibernéticas do Brasil.

Para isso, este trabalho foi dividido em três capítulos que abordam sobre a questão cibernética e as estratégias dos países analisados. O primeiro capítulo é subdividido em três partes, em que a primeira conta com um breve histórico sobre a criação e formação da internet e a emergência de novas ameaças relacionadas ao ciberespaço. A segunda parte apresenta uma discussão terminológica sobre os conceitos de defesa e segurança nacional, incorporando esses conceitos para a questão da defesa e a segurança cibernética. A terceira parte desse capítulo traz uma introdução ao ciberespaço, seus conceitos e implicações nas relações entre atores estatais e não estatais.

O segundo capítulo consiste na análise das estratégias nacionais cibernéticas de Estados Unidos, China e Israel, buscando entender os principais objetivos e fatores estratégicos entre as visões de cada país em relação ao ciberespaço e a sua defesa e segurança. O terceiro e último capítulo traz uma análise sobre a compreensão do Brasil sobre o ciberespaço e o setor cibernético, em conjunto com uma discussão crítica sobre os quatros países, buscando assimilar as aproximações e os distanciamentos entre eles com a finalidade de verificar a hipótese de o modelo cibernético brasileiro sofrer influência das estratégias das três potências cibernéticas analisadas. Por fim, uma conclusão com as considerações finais obtidas a partir do que foi exposto.

2 O CIBERESPAÇO E A SEGURANÇA INTERNACIONAL

Neste primeiro capítulo serão abordadas questões teóricas e conceituais envolvendo o ciberespaço. Por ser considerado um novo domínio de poder na política internacional, ainda há muitas incertezas sobre como esse ambiente pode impactar a segurança internacional e as relações internacionais como um todo. Por isso, este capítulo tratará sobre como o espaço cibernético tem questionado as visões tradicionais sobre o Estado e a sua soberania, assim como abordar sobre como as novas ameaças, possibilitadas pelo ciberespaço, podem afetar a segurança internacional.

2.1 Breve histórico da Internet e a emergência de novas ameaças

Em um contexto de Guerra Fria entre Estados Unidos e União Soviética, as duas maiores potências mundiais da época, a corrida armamentista e tecnológica propiciava o desenvolvimento de equipamentos que beneficiavam o domínio político, militar e econômico de uma potência sobre a outra. Nesse período, mais especificamente em 1958, o projeto *Advanced Research Projects Agency* (ARPA) foi fundado pelos estadunidenses, na tentativa de unir uma quantidade de computadores e estabelecer uma rede na qual os pesquisadores conseguiriam usá-la de forma cooperativa, permitindo a comunicação entre os computadores e facilitando o uso remoto de programas (RYAN, 2010). Esse projeto mais tarde passou a ser chamado de “ARPANET” e teve sua primeira transmissão efetiva em 1969.

Com o resultado positivo da comunicação entre os computadores da agência através de nódulos da rede criada, na década de 70 foi decidido que o projeto deveria ser expandido para o setor espacial, em vista da intensificação do envio de satélites no período (RYAN, 2010). O objetivo era conectar os satélites através de uma rede em comum e a ARPA passou a desenvolver a possibilidade fundando a rede de satélites do Atlântico, denominado em 1975 de “SATNET”. Dessa forma, ao final da década de 1970, o projeto já havia construído três redes em funcionamento, a “ARPANET”, a “PRNET” e a “SATNET”, utilizando cabos, radio e satélite, respectivamente (RYAN, 2010). Entretanto, a rede apenas permitia a comunicação restrita entre os computadores determinados para a construção e uso das redes pelo projeto.

“O sistema consistia na tecnologia de troca de pacote de dados e informações por meio de uma rede independente de centros de comando e controle, dessa forma a mensagem buscava suas próprias rotas pela rede” (CASTELLS, 1999 apud FERREIRA, 2017, p. 26). Ou seja, as informações seriam transmitidas de maneira mais segura e rápida. A rede ainda não podia ser

considerada como a internet que conhecemos hoje, sendo que foi apenas no fim da década de 1980 que a rede deixou de ser exclusividade das forças armadas dos Estados Unidos. Isso ocorreu quando a "NSFNET" foi criada, por meio da *National Science Foundation*, agência governamental norte americana de pesquisa científica. Ela foi conectada ao "ARPANET" utilizando-se de seu protocolo TCP/IP e deu início ao processo de transição do uso da rede exclusiva de militares para os civis (RYAN, 2010). Pode-se dizer que a "NSFNET" possuía as características iniciais da internet que conhecemos hoje e começou a se espalhar rapidamente pelo território norte americano.

"Em outubro de 1991 cerca de 620 mil computadores estavam online e dois anos depois, em outubro de 1993, mais de dois milhões de computadores estavam conectados à internet" (RYAN, 2010, p. 94). A conectividade e comunicação na internet se dava por meio das correspondências eletrônicas (e-mails) e foi a primeira plataforma global de rede cruzada. A "NSFNET" começou a se interligar com outras redes existentes entre centros de pesquisas e universidades em todo o mundo, sendo principalmente utilizada como um mecanismo de compartilhamento de informações no ambiente acadêmico (MONTEIRO, 2001).

Foi também na década de 90 que o *World Wide Web* (WWW) veio à tona, um projeto de Tim Berners-Lee na CERN (Conselho Europeu para Pesquisa Nuclear) que alterou a maneira como os humanos interagem e realizam as suas funções, sejam elas básicas ou especializadas. O objetivo era criar um sistema que se utilizaria de frases e letras em um documento de hipertexto que poderiam ser vinculadas a outras informações (MONTEIRO, 2001). O hipertexto desenvolvido foi o *HyperText Markup Language* (HTML), uma linguagem de programação que podia adicionar em um servidor da Web qualquer tipo de informação, fosse ela em formato de texto, imagem ou arquivo (FERREIRA, 2017). "A WWW pode ser considerada a mais significativa e célebre manifestação das Tecnologias de Informação e Comunicação" (MIRANDA, 2007, p. 3).

Desse momento em diante, a internet se difundiu de modo exponencial pelo mundo, se tornando uma ferramenta social, e não apenas militar e acadêmica. "A internet agora se tornou quase que um serviço "comódite", e muito da atenção dada recentemente tem sido sobre o uso dessa infraestrutura da informação global para o suporte de outros serviços comerciais" (LEINER et al. 2009, p. 30, tradução nossa)[1]. A princípio, a sua estrutura era gerenciada pelo governo dos EUA, em coordenação com o Departamento de Defesa, apesar de não haver um controle centralizado sobre a rede. Contudo, a expansão da internet fez com que a dificuldade

[1] Texto original: The Internet has now become almost a "commodity" service, and much of the latest attention has been on the use of this global information infrastructure for support of other comercial services.

de sua coordenação e os interesses comerciais com o seu uso se tornassem insustentáveis para o setor público. O senador Al Gore lutava pela sua privatização desde 1990, até que em 1994, quando era Vice Presidente, a *National Science Foundation* transferiu o controle das conexões para interesses privados (SINGER; FRIEDMAN, 2013).

Em 1998, o Departamento de Comércio dos EUA propôs a fundação de uma nova corporação sem fins lucrativos que tomaria o controle do Sistema de Nomes e Domínio (DNS). No intuito de operar para o benefício da comunidade da internet como um todo, a nova corporação foi chamada de *Internet Corporation for Assigned Names and Numbers* (ICANN), que obteve a sua total independência do governo norte americano apenas no ano de 2009, onze anos após a primeira assinatura do memorando de entendimento entre a corporação e o Departamento de Comércio (RYAN, 2010). Até os dias de hoje, a ICANN permanece sendo responsável pela atribuição de endereços de IP (Protocolo da Internet), identificadores de protocolo e pela administração dos seus domínios.

No século XXI o número de usuários na rede mundial atingiu os patamares mais elevados até então, segundo o Internet World Stats[2], em 30 de junho de 2019 a internet registrou 4,5 bilhões de usuários no mundo, um percentual de 58.8% da população mundial. Para noção de comparação, conforme o mesmo site, no ano de 2000 esse número era de cerca de 360 milhões de pessoas ao redor do planeta, o que representa um crescimento expressivo e exponencial em duas décadas. Esse crescimento reflete o desenvolvimento de todo um ecossistema que a internet proporcionou, impactando na geração de novos empregos, redução de custos, facilidade de acessos a produtos, serviços e mão de obra, tornando possível que países em todo o globo pudessem investir em conhecimentos na área das TICs, criando um ambiente de competição e cooperação entre os países (OLIVEIRA, 2014 *apud* FERREIRA, 2017).

Todas as mudanças geradas a partir da criação da internet e o seu amplo uso ao redor do mundo fizeram com que novas ameaças e vulnerabilidades se tornassem parte do dia a dia da humanidade e, em consequência, das nações. Ocorreu a digitalização de equipamentos e tarefas que antigamente eram manuais e exigiam, muitas vezes, um desgaste físico e uma grande quantidade de tempo para que fossem realizadas, modificando os modos de produção. No entanto, ao mesmo tempo que tornou a realização de muitas tarefas mais práticas, também aumentou a vulnerabilidade dos setores que se digitalizaram, visto que a normalidade das operações e trabalhos agora são dependentes do funcionamento correto dos equipamentos e dos seus sistemas digitais.

[2] Disponível em: https://www.internetworldstats.com/stats.htm

Dessa forma, percebe-se uma interdependência entre o mundo digital, que tem o ciberespaço como ambiente de funcionamento, e o mundo humano material, representando um risco não apenas à esfera informacional, mas também para estruturas vitais (MARTINS, 2012). “A conexão de toda esta interdependência origina a possibilidade de colocar em causa e em risco não só informação irrelevante, mas, sobretudo, dados estratégicos e vitais do Estado à sociedade civil” (MARTINS, 2012, p. 46). As ameaças que emergem, portanto, dizem respeito ao estado de instabilidade que um ataque cibernético ou o uso indevido do espaço virtual pode causar a segurança nacional e internacional.

Segundo a União Internacional de Telecomunicação (UIT) (2008), essas novas ameaças podem incluir sabotagem, vandalismo, mal configuração do sistema, negação de serviço, espionagem, vasculho de informações, roubo de serviço, entre outros. A tabela a seguir ilustra algumas das ameaças provindas do ciberespaço, indicando seus principais alvos, estatais e não estatais.

Figura 1 - Ameaças cibernéticas

Ameaças	Definição Securitária	
Hacktivismo	CIBERSEGURANÇA	Alvo principal é a área Privada/Sociedade Civil
Crime Cibernético		
Espionagem Cibernética	CIBERSEGURANÇA / CIBERDEFESA	Alvo principal é tanto a área Privada/Sociedade Civil como o setor Público
Sabotagem Cibernética		
Terrorismo Cibernético	CIBERDEFESA	Alvo principal é o setor público e suas infraestruturas criticas
Guerra Cibernética		

Fonte: AYRES PINTO; FREITAS; PAGLIARI, 2018.

Joseph Nye Jr (2017) vai além dessa interpretação e também configura a ruptura do sistema digital como uma ameaça à privacidade dos indivíduos e um risco ao Estado. Por conseguinte, argumenta que os atores, estatais e não estatais, devem estar cientes dos riscos que envolvem o ciberespaço, reconhecendo que um inimigo pode explorar suas vulnerabilidades para cometer atos que comprometam a sustentabilidade dos seus sistemas e tecnologias.

Em relação ao terrorismo cibernético, por exemplo, a possibilidade de disseminação de informações por qualquer pessoa, com baixos custos e em grande parte sem controle do conteúdo disseminado, faz da internet um espaço propicio para a promoção de ideias e ataques

terroristas (BRUNST, 2010). O termo terrorismo possui variadas definições e interpretações. Consequentemente, o termo ciberterrorismo também não tem uma conceituação clara e específica, podendo ser referido, de modo limitado, como "ataques politicamente motivados contra sistemas de informação que resultam em violência contra alvos não combatentes" (POLLITT, 1998 *apud* BRUNST, 2010, p. 51).

A questão é que a internet possibilita que ataques possam ser efetuados sem a presença física do "ciberterrorista", pois não há limites materiais para que as agressões sejam feitas, tornando o ambiente virtual mais vantajoso do que ataques convencionais (BRUNST, 2010). Ademais, é uma ferramenta que pode ser favorável para a propagação do medo e dos ideais dos grupos terroristas, já que se pode atingir um maior número de pessoas dado que os fluxos de informações no espaço cibernético são maiores.

Em vista disso, de acordo com o relatório da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) "*Cybersecurity Policy Making at a Turning Point* (2012)", uma onda de políticas governamentais está sendo confeccionada por diversos países para enfrentar os desafios da segurança cibernética, entre eles, os países abordados neste trabalho: Estados Unidos, China e Israel. O questionamento sobre como melhor se preparar e se adaptar ao mundo e ao futuro digital é algo que está sendo encarado como um desafio aos Estados, que estão passando a enxergar a questão cibernética como determinante para a ordem socioeconômica e política dos países (HADDAD; BINDERS, 2019).

O problema reside justamente no fato de que as ameaças digitais tendem a aumentar com a digitalização da sociedade e os métodos convencionais de segurança não serão eficazes contra tais ameaças (HADDAD; BINDERS, 2019). Por conseguinte, os ataques cibernéticos passaram a ser vistos como atos que possuem o potencial de principiar conflitos e uma possível guerra cibernética, com consequências físicas.

Foi o que John Arquilla e David Ronfeldt teorizaram em 1993, sendo os responsáveis por introduzir o termo "*Cyberwar*" (ciberguerra) aos Estudos de Segurança, Defesa e Estratégia, em seu artigo "*Cyberwar is Coming!"*. Os autores definem a guerra cibernética como [...] "a condução e a preparação para a condução de operações militares, de acordo com princípios relacionados com a informação" (ARQUILLA; RONFELDT, 1997, p. 30, tradução nossa)[3]. Mudanças na maneira de enxergar a guerra, assim como a própria natureza dos conflitos com os avanços tecnológicos foi colocado em pauta. "A informação está se tornando um recurso estratégico, que pode se mostrar tão valioso e influente para Era Digital quanto o capital e o

---

[3] Texto original: [...] conducting, and preparing to conduct, military operations according to information-related principles.

trabalho têm sido para a Era Industrial" (ARQUILLA, RONFELDT, 1997, p. 25, tradução nossa)[4]. Nesse sentido, os aspectos da fácil entrada ao ambiente virtual pelas suas poucas barreiras, assim como o seu baixo custo, tornam atraente o uso do setor cibernético como arma em um possível conflito.

Ainda sem conceituação internacional oficial, as armas cibernéticas podem ser conceituadas como:

> [...] meios cibernéticos de guerra que são projetados, usados, ou sua intenção de uso é capaz de causar (i) dano ou morte a pessoas; (ii) deterioração ou destruição de objetos; isso é, causando as consequências requeridas para qualificar uma operação cibernética como um ataque (MANUAL DE TALLINN, 2013, p. 119, tradução nossa)[5].

Em relação à guerra cibernética que o uso dessas armas pode ocasionar, Clarke e Knake (2010) a definem como "ações cometidas por um Estado-nação para penetrar a rede de computadores de outra nação com o propósito de causar danos ou perturbações" (CLARKE; KNAKE, 2010, p. 9, tradução nossa)[6]. Com isso, apesar de atitudes cibernéticas ofensivas ainda não terem representado uma participação crucial em um grande conflito, a comunidade internacional já reconhece a importância do tema para a segurança e a defesa nacional dos Estados, que se veem na posição de ter que repensar as suas estratégias e seus modos de lutar guerra.

Um dos mais famosos ataques cibernéticos do século XXI ficou conhecido como *Stuxnet,* ocorrido em 2010 no Irã. O episódio consistiu na implementação de um malware, uma espécie de software maligno, nas facilidades nucleares do Irã e tinha como objetivo prejudicar o enriquecimento de urânio do país. O malware conseguiu danificar o processo de enriquecimento por fazer com que os rotores de centrifugação funcionassem de maneira anormal, acelerando e reduzindo drasticamente as suas velocidades, causando vibrações que ou iriam destruir as centrífugas ou danificá-las drasticamente (VALO, 2014). O malicioso programa utilizado no caso *Stuxnet* é considerado de alta sofisticação e foi o primeiro caso em que um ataque cibernético afetou de maneira direta o funcionamento de estruturas físicas, prejudicando o enriquecimento de urânio por parte do Irã.

---

[4] Texto original: Information is becoming a strategic resource that may prove as valuable and influential in the post-industrial era as capital and labor have been in the industrial age.

[5] Texto original: [...] cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as na attack.

[6] Texto original: actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage of disruption.

Isto posto, a forma como a comunidade internacional lida com incidentes cibernéticos como esse é subjetiva, não há respostas claras nem métodos delineados a serem seguidos, evidenciando as dificuldades que os Estados encontram em atribuir e retaliar os responsáveis por ataques virtuais. Sendo assim, o ciberespaço permite que mesmo que um adversário seja menos capacitado em recursos tradicionais de guerra, ainda assim pode confrontar um oponente visivelmente superior, pois apesar da força reduzida, é capaz de provocar danos (FERREIRA, 2017). Isso significa que Estados considerados mais fracos, ou mesmo indivíduos, podem se beneficiar dessa assimetria, especialmente no que concerne ao anonimato e a dificuldade em localizar o agressor (NYE, 2010). Os indivíduos com ações ativas e que executam agressões virtuais são denominados *hackers*, que podem ser definidos como invasores de computadores que penetram em banco de informações públicas ou privadas por satisfação própria em busca de reconhecimento (KAPTO, 2013),

Com relação a isso, Clarke e Knake (2010) analisam que esses fatores podem criar obstáculos e constrangimentos para as ações dos Estados:

> A menos que reduzamos nossas vulnerabilidades a ataques cibernéticos, sofreremos auto-dissuasão. Nosso conhecimento sobre o que os outros podem fazer conosco pode criar uma situação na qual relutamos para utilizar nossa superioridade em outras áreas, como armas convencionais, em situações em que nosso envolvimento, para nós, pode ser justificado. As armas cibernéticas de outras nações podem nos impedir de agir, não apenas no ciberespaço, mas em outros meios também. (CLARKE and KNAKE, 2010, p.77, tradução nossa)[7]

A cibersegurança já não é um assunto novo no âmbito da segurança internacional, mas precisa ser aprimorado, não há dimensões bem estabelecidas quanto aos seus possíveis efeitos para as nações. O relatório *Global Risks Report* (2019), do Fórum Econômico Mundial, elencou ataques cibernéticos entre os dez maiores riscos globais para a humanidade em termos de impacto, configurando-os como a maior ameaça no que concerne à categoria de tecnologia, conforme a metodologia utilizada no relatório.

> Os ataques e as ameaças podem afetar e interromper a estrutura de funcionamento e os recursos de defesa de um Estado, em especial contra recursos informatizados responsáveis pelo controle e gerenciamento de equipamentos militares, que integram os sistemas de comando e controle (OLIVEIRA, 2011, *apud* PORTELA, 2015, p. 28).

Assim sendo, o ambiente cibernético também afeta a defesa nacional de um país, ligado a ataques externos ao território nacional, e que, por não ter fronteiras definidas, aumenta

[7] Texto original: Unless we reduce our vulnerabilities to cyber attack, we will suffer from self-deterrence. Our knowing about what others could do to us may create a situation in which we are reluctant to use our superiority in other areas, like conventional weapons, in situations where it might be warranted for us to get involved. Other nations' cyber weapons may deter us from acting, not just in cyberspace but in other ways as well.

a complexidade de compreensão dos atos que transgridem os limites da nação. Nesse contexto, é preciso analisar de forma mais elaborada as distinções terminológicas entre segurança e defesa, adaptando o seu uso para a questão cibernética.

2.2 Terminologia de Defesa e Segurança Cibernética

Existe certa falta de clareza na distinção entre os termos segurança cibernética e defesa cibernética. Apesar de possuírem referenciais diferentes, no qual cada um compreende um âmbito dentro do ciberespaço, há muitas vezes uma confusão quanto aos seus significados. Para se compreender a divergência entre segurança e defesa cibernética, é preciso primeiro assimilar os conceitos clássicos de segurança e defesa, que acabam englobando diversas variações e complicando o entendimento geral sobre o assunto.

Em 1994, a Organização das Nações Unidas (ONU), por meio do relatório "*Human Development Report*", do Programa de Desenvolvimento das Nações Unidas (PNUD), ampliou o conceito de segurança no contexto internacional, passando a englobar o indivíduo como sujeito e expandindo uma visão que era centralizada no Estado. Com isso, os objetos de estudo de segurança começaram a incluir aspectos de ordem econômica, ambiental, política e de saúde, por exemplo. Em um contexto anterior, no período da Guerra Fria, os estudos de segurança estavam centrados em assuntos militares, os assuntos e problemas que não envolviam as forças militares ou que simplesmente não eram consideradas relevantes, eram categorizados de baixa política (BALDWIN, 1997).

De acordo com Barry Buzan (1997), a visão tradicional de que apenas os assuntos militares valiam para a agenda de segurança começou a sofrer erosão com o desaparecimento contínuo de guerras interestatais, dando vazão para que fosse dado importância para questões de outras naturezas. Com isso, Buzan (1997) propõe que a securitização, ou seja, o ato de tornar uma área em uma questão de segurança, deve ser compreendida como um processo intersubjetivo. Dessa forma, englobar o âmbito cibernético como um fator securitário ocorre em vista da relação entre a proteção de informações consideradas estratégicas, principalmente ligadas a infraestruturas críticas de informações, e o funcionamento estável e normal do Estado.

Pode-se definir a segurança, de maneira abrangente, como "um estado de equilíbrio, onde os indivíduos possuem a percepção de liberdade para o acesso a informações, produtos e processos que consideram apropriados para fomentar o seu desenvolvimento [...]" (RAZA,

2005, p. 69, tradução nossa)[8]. É possível entender que a segurança, portanto, refere-se aos fatores que contribuem para a estabilidade interna da nação e o seu objetivo é a proteção desses fatores, principalmente os considerados estratégicos, para garantir o bem estar da população e o funcionamento regular das instituições.

No Brasil, a Escola Superior de Guerra (ESG) em seu Manual Básico, define o termo segurança como “[...] a sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza” (ESG, 2014, p. 76). Sendo assim, a identificação das ameaças e vulnerabilidades é vista como crucial dentro da política de segurança nacional, pois com isso os Estados podem limitar ou conter as suas inseguranças por meio da diminuição de suas vulnerabilidades ou enfraquecendo as fontes de ameaças (GOLDMAN, 1982 *apud* RUDZIT; NOGAMI, 2010).

Em contrapartida, a defesa nacional possui o seu cerne nas ameaças externas que um país pode sofrer, sendo diretamente ligado às funções das Forças Armadas, mas não exclusivamente, para a proteção do território e da soberania nacional. Como ilustra o embaixador peruano José Antonio Bellina Acevedo:

> [...] uma resposta definitiva afirmaria que a segurança compete ao ambiente interno e, portanto, exclusivamente às forças policiais ou às forças de segurança e a defesa unicamente ao plano externo, e, por assim ser, faz-se da competência das forças armadas (ACEVEDO, 2008, *apud* BENTO, 2013, p. 121).

Seguindo uma ideia semelhante, o Plano Nacional de Defesa (PND) (2012) do o Ministério da Defesa (MD) do Brasil adota que a defesa nacional é “o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantes externas, potenciais ou manifestas.” (MINISTÉRIO DA DEFESA, 2012a, p. 15).

Isso significa que conceito de defesa pode abranger todos os recursos materiais, humanos, organizacionais e informacionais que um Estado pode utilizar para se proteger de ataques externos e insurgências domésticas, sendo o seu principal instrumento, mas não limitado a ele, as Forças Armadas. (RAZA, 2005). Desse modo, a separação entre segurança e defesa pode ser notada através dos atores e instituições responsáveis por estabelecer cada seguimento a partir de suas funções. Os desafios, ameaças e preocupações são muitas vezes distintos para cada área, atingindo diferentes aspectos estatais, assim como as políticas a serem aplicadas para que tanto a segurança quanto a defesa nacional sejam garantidas no país.

---

[8] Texto original: state of equilibrium where individuals perceive themselves as having the freedom to access information, products and processes they consider proper for fostering their development.

Com os conceitos e definições apresentados, é possível enquadrar os entendimentos dos termos acerca da segurança e defesa para o âmbito cibernético. Para o Departamento de Defesa dos Estados Unidos, por exemplo, a defesa cibernética se refere à "ações tomadas para proteger o ciberespaço de ameaças que podem violar as medidas de segurança no espaço cibernético e inclui medidas para detectar, caracterizar, conter e mitigar essas ameaças, incluindo malware ou atividades não autorizadas, de forma a restaurar o sistema para a sua configuração segura". (DOD, 2020, p. 56, tradução nossa)[9]

Por sua vez, para o general Paulo Carvalho (2011), que já foi chefe do Centro de Defesa Cibernética (CDCiber) do Brasil, a defesa cibernética consiste em ações defensivas, exploratórias e ofensivas realizadas no ciberespaço com a finalidade de proteger os sistemas de informação, dentro de um contexto de planejamento militar. A visão de Carvalho insere a defesa cibernética ao setor militar, sendo este o responsável pelas dimensões táticas, operacionais e estratégicas, principalmente no emprego de ações consideradas exploratórias e ofensivas, que envolvem a obtenção de dados para a produção de conhecimento de inteligência e a promoção de prejuízos aos sistemas de informação de oponentes.

Já a segurança cibernética, Carvalho (2011) aponta como a proteção e garantia do uso de ativos de informação estratégicos, em especial redes de comunicação, computadores e sistemas informatizados responsáveis pelo controle das infraestruturas críticas nacionais, no qual muitas vezes envolve a interação entre órgãos públicos e privados para o seu funcionamento. Isso significa que a cibersegurança pode ser definida como "medidas que visam assegurar o bem-estar e o regular ordenamento de uma nação no ciberespaço e fora dele, desde que o ordenamento fora do espaço cibernético seja decorrente de ações diretamente ligadas a ele". (MILITÃO, 2014, p. 26)

Essas definições convergem com o entendimento do Departamento de Defesa norte americano, que considera a segurança cibernética como "ações tomadas para a proteção do ciberespaço, a fim de prevenir acessos não autorizados, exploração e/ou danos a sistemas eletrônicos de comunicação e outras tecnologias da informação, incluindo plataformas de tecnologias da informação, assim como as informações contidas nelas, de maneira a garantir a

[9] Texto original: Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, conter, and mitigate threats, including malware or the unauthorized activities of users, and to resolve the system to a secure configuration.

sua integridade, autenticidade, confidencialidade. viabilidade e não repúdio" (DOD, 2020, tradução nossa)[10].

Assim como os termos originários de defesa e segurança, a ciberdefesa e a cibersegurança comportam diferentes esferas. Cada qual com um domínio característico de atuação no ciberespaço, enquanto o primeiro trata de assuntos concernentes a relações interestatais, como o poder cibernético, o segundo corresponde à dimensão da segurança pública, como a proteção do meio cibernético (FERREIRA, 2017).

2.3 Ciberespaço: definição, características e impacto no sistema internacional

Visto a questão terminológica e o contexto histórico da internet e a suas ameaças, podemos partir para uma análise mais específica sobre o ciberespaço e o que ele representa hoje para o sistema internacional. Primeiro, é preciso compreender a importância da dominação de espaços e da determinação dos seus limites para as relações humanas.

Pode-se interpretar que barreiras físicas restringem e impõem limites às ações e atividades humanas, sejam restrições de origem natural ou construídas pelo próprio ser humano, de maneira a aprimorar ou até mesmo dificultar o seu modo de vida. Na história da humanidade, tais limites foram muitas vezes motivadores para a conquista de territórios, em que a preservação desses territórios influenciou de maneira direta a nossa evolução como sociedade. O conceito de Estado perpassa justamente pelos limites físicos territoriais em que uma população está estabelecida, possuindo e exercendo soberania sobre esse território (RAFFESTIN, 1993). O espaço virtual, entretanto, formado a partir das inovações tecnológicas e do aprimoramento das redes de comunicação no mundo, por não ter barreiras materiais, trouxe novos horizontes para se compreender as relações humanas e consequentemente, as relações internacionais (MARTINS 2012).

A visão tradicional de fronteira, segundo Ratzel (1987), se fundamenta na caracterização de fronteiras políticas, naturais e artificiais, que de modo geral referem-se à espaços físicos ou naturais nos quais a humanidade foi tomando as suas ações ao longo da sua história, com base em fatores políticos, culturais e de segurança (RATZEL, 1987 *apud* SEABRA, 2012). Dessa forma, a demarcação de limites como grandes muros em vilas e cidades durante o período feudal, por exemplo, demonstra a necessidade humana de obter segurança e

[10] Texto original: Actions taken within protected cyberspace to prevent unauthorized accesss to, exploitation of, or damage to computers, eletronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidenciality, and nonrepudiation.

deter controle sobre determinado local. Nessa época, além dos muros externos, havia também uma segregação em relação ao castelo do senhor feudal, que era defendido por grossas muralhas (LOPES; NETO, 2015).

Por sua vez, o ambiente digital, virtual e invisível, utilizado a partir do uso de tecnologias eletrônicas, se caracteriza por possuir fronteiras que não se adequam a essa visão tradicional. Sua demarcação é materialmente intangível e nele o fluxo e a interação de informações e dados ocorrem de maneira intensa. Esse ambiente passou a ser chamado de ciberespaço, ou espaço cibernético, e pode ser definido como [...] "o reino das redes de computadores (e dos usuários por trás deles) no qual as informações são armazenadas, compartilhadas e comunicadas de maneira online" (SINGER; FRIEDMAN, 2013, p. 13, tradução nossa)[11].

Essa natureza transfronteiriça faz com que emerjam novas percepções em relação a conceitos tradicionais de dimensões de poder, domínio territorial e soberania. A partir da conceituação de Weber, o Estado é "uma comunidade humana que pretende, com êxito, o monopólio do uso legítimo da força física dentro de um determinado território" (WEBER, 1982, p. 98). Dessa forma, a delimitação de fronteiras converge com a autoridade que determinado Estado desempenha sobre um território. O ciberespaço, entretanto, se configura como um ambiente de fronteiras invisíveis e a sua delimitação pode ser vista como um desafio para os governos nacionais.

Caracterizado por afetar de maneira variada as condutas humanas, segundo Martins (2012), o espaço cibernético estimula uma mudança no comportamento cultural e social por permitir uma grande velocidade dos fluxos de informações, por ser transnacional por natureza e não possuir autoridade central reguladora. É assumido, portanto, que assim como os dispositivos tecnológicos alteram a nossa maneira de viver em sociedade, também podem afetar a interação entre os atores nas relações internacionais.

Além disso, esse novo espaço também consiste em uma rede de infraestruturas de TICs, incluindo a internet, redes de telecomunicação, sistemas de computação, processadores e computadores, que o torna dependente de espaço físico e de ferramentas materiais. Ou seja, o espaço cibernético não pode ser considerado exclusivamente virtual e imaterial, pois sua existência está vinculada às raízes de servidores que se encontram em território físico, fazendo com que o controle desses servidores, por determinado país, possa ser visto como uma questão de soberania nacional (KHANNA, 2018).

[11] Texto original: [...] the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online.

Conforme visto, a legitimação do uso do poder pelo Estado ocorre por meio do domínio territorial e do reconhecimento de sua soberania nacional. Consequentemente, o ciberespaço tem sido reconhecido na política internacional como um quinto domínio de poder, além dos outros tradicionais domínios: terra, água, ar e o espaço. Contudo, não há governança sobre o espaço cibernético e, por conseguinte, os governos são os responsáveis por promulgar leis nacionais em relação à segurança cibernética, agindo da forma como enxergam o ciberespaço, pois não existe uma regulamentação que guie e/ou constranjam o comportamento dos países nesse espaço (ELSTRUP, 2018).

Dessa maneira, "o ciberespaço tem a capacidade de desafiar a soberania nacional, visto que pode questionar a habilidade do Estado em regular os movimentos e os fluxos de informações dentro de suas fronteiras nacionais" (KHANNA, 2018, p. 140, tradução nossa)[12]. Esses fluxos de informações e dados virtuais cruzam fronteiras terrestres em questão de milésimos de segundos, resultando em uma grande dificuldade para filtrar o seu conteúdo, podendo ser visto como um aspecto que pode perturbar sistemas políticos (MARTINS, 2012).

Consequentemente, segundo Nye (2010), atingir o controle sobre o domínio cibernético como os Estados possuem em relação aos domínios tradicionais é improvável, pois o ciberespaço se configura como um domínio de difusão de poder, em que além do controle do fluxo de informações ser difícil, as barreiras de entrada ao mundo cibernético são baixas, permitindo que indivíduos, Estados fracos e pequenos e atores não estatais consigam ter participação ativa.

O demasiado uso da internet pela humanidade é o retrato disso, demonstrando uma dependência digital construída nos últimos anos. "A forma como as pessoas produzem, consomem, comercializam, como se comunicam, interagem e agem politicamente e profissionalmente em suas vidas particulares são afetadas por essas tecnologias e infraestruturas" (HERCHEUI et al., 2012, p. 2, tradução nossa)[13]. Em conjunto com o fenômeno da globalização e a consequente interdependência entre os países, portanto, a dimensão tecnológica afetou a dimensão humana e social, proporcionando uma mudança substancial no mundo, na realidade na qual o ser humano está inserido e como ele interage com o ambiente externo (MARTINS, 2012).

---

[12] Texto original: Cyberspace is also capable of challenging state sovereignty, since it can question the state's ability to regulate movement across borders.

[13] Texto original: How people produce, trade and consume goods and services, and how people communicate, Interact and collaborate in their political, professional and private lives are all affected by these technologies and infrastructures.

Isso ocorre devido a possibilidade de um indivíduo assumir novas identidades no mundo virtual, com novas funções a serem desempenhadas, moldando a realidade na qual se vê imerso - mesmo que de modo indireto e involuntário – e isso acaba sendo projetado para a realidade internacional. (MARTINS, 2012). Pois, com isso, os Estados passam a buscar o desenvolvimento de capacidades para lidar com as vulnerabilidades e ameaças que essas novas formas de interação possibilitam, no intuito de manter a estabilidade social, econômica e política das nações.

A difusão de poder comentada por Nye (2010) tem suas justificativas centradas principalmente na forma como utilizamos o ciberespaço em nossas vidas. O fácil acesso ao mundo das informações possibilita interações impensáveis há 50 anos atrás e a sua difícil delimitação territorial o torna um espaço propício para a projeção de poder. Segundo o autor, mudanças nas formas de disseminar informações sempre tiveram um importante impacto nas relações de poder e, nesse caso, o ciberespaço faz com que os Estados, principalmente as maiores potências mundiais, não possuam o mesmo controle que possuem sobre os outros domínios tradicionais.

Desse modo, Nye (2010) chama esse poder de *cyberpower* e o define de duas maneiras. A primeira refere-se à questão comportamental e consiste na habilidade de obter resultados por meio de recursos de informações eletronicamente interconectados do domínio cibernético. A segunda diz respeito a habilidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais por meio de instrumentos de poder. Apesar da difusão que o ciberespaço permite, o autor argumenta que o Estado ainda prevalece como o principal ator das relações internacionais, pois é detentor de mais recursos e das maiores capacidades de controle. Consequentemente, apesar de difundir o poder, o ciberespaço não o torna igualitário entre os atores, mantendo o *status quo* de um ambiente assimétrico (NYE, 2010).

Com uma participação mais ativa da população tendo acesso ao poder que a informação oferece, os governos tendem a modificar o uso das tecnologias da informação para manter o controle sobre o domínio cibernético. Nye (2010) analisa que os governos nacionais sempre estiveram preocupados com a disseminação e o controle de informações. Meios de comunicação sempre foram perseguidos durante regimes autoritários justamente por ameaçar, mesmo que de maneira indireta, a manutenção do poder.

Além disso, os novos tipos de ataques e agressões que podem ser efetuados entre os atores devido ao mundo cibernético, como já comentado neste capítulo, demonstra que apesar das vantagens, a dependência digital também trouxe fragilidades. A anarquia, representada na

ausência de uma regulamentação internacional em relação ao ciberespaço e o seu uso pelos países, faz com que os Estados possam lidar com o espaço cibernético a partir das suas próprias concepções de como isso afeta a sua segurança nacional. Não há definições claras no direito internacional de atos que podem ser considerados como atos de guerra no ciberespaço, por exemplo, dificultando a distinção entre ações hostis e erros, de forma a criar uma falta de clareza sobre o que constitui um ataque cibernético e sobre quais comportamentos podem ser considerados legais ou ilegais (EILSTRUP-SANGIOVANNI, 2018).

Com isso, a segurança cibernética, definida pela UIT como:

> [...] coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de riscos de gerenciamento, ações, treinamentos, boas práticas e tecnologias que podem ser utilizadas para proteger o ambiente e organização cibernética e os recursos dos usuários (UIT, 2008, p. 2, tradução nossa)[14]

Acaba se confirmando como um importante fator para a garantia da segurança e dos interesses nacionais. Pois, dado que as tecnologias da informação e comunicação afetam os comportamentos sociais, políticos e econômicos do mundo, o seu funcionamento correto e sustentável, assim como a sua utilização, passam a ser reconhecidos como elementos essenciais para o andamento seguro de uma nação.

Atualmente, o funcionamento de diversos setores considerados imprescindíveis para a sociedade moderna está diretamente ligado ao setor cibernético. O ambiente digital se tornou o principal meio para as relações financeiras, sociais, acadêmicas e para o funcionamento do sistema de comunicação, transporte, energia, entre outros (HERCHEUI, 2012). As infraestruturas responsáveis por possibilitar o funcionamento desses setores imprescindíveis são vistas como infraestruturas críticas de um país, que podem ser definidas como "[...] recurso vital ou centro gravitacional no qual a sua destruição pode causar um gigantesco efeito sobre a segurança nacional e na capacidade do Estado em operar normalmente" (SALTZMAN, 2013, p.43, tradução nossa)[15]. Dessa forma, políticas de segurança cibernética emergem ao redor do mundo e ganham cada vez mais notoriedade, já que as suas aplicabilidades são cada vez mais importantes para a preservação da harmonia na sociedade.

Outro importante aspecto da segurança cibernética diz respeito TICs, principais componentes do novo domínio, que provém em sua grande maioria do setor privado. Em muitos países, como os EUA, o setor privado é responsável majoritariamente pela produção de

---

[14] Texto original: [...] collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber enviroment and organization and user's assets.

[15] Texto original: [...] vital or centre-of-gravity assets whose destruction may have a colossal effect on a state's national security and its capacity to operate normally.

infraestruturas e tecnologias, enquanto que o governo fica com a responsabilidade de incentivar e delinear as diretrizes e estratégias para a área cibernética (CHUNG, 2019).

Logo, evidencia-se a necessidade de uma coordenação entre o setor público e o setor privado para a efetividade das ações de segurança cibernética. Os atores políticos precisam tomar decisões com base em avaliações precisas sobre os riscos, ameaças e vulnerabilidades que todo o ecossistema da cibernética possui, pois o ciberespaço é complexo, disperso e interconectado com os mais diversos setores institucionais (CHUNG, 2019).

Correlacionando os fatores de segurança e as relações de poder, a evolução tecnológica também possibilitou um maior potencial econômico e militar no mundo, principalmente nas grandes potências. Segundo Ferreira (2017), no sistema internacional o uso da força e da tecnologia estão envolvidos numa forte relação. Por conseguinte, a capacidade de domínio e controle de um país sobre novas tecnologias se tornou vital na distribuição do poder entre os países no mundo.

Assim, a análise dessa distribuição atualmente precisa levar em consideração o fator tecnológico. No sistema econômico capitalista, o conhecimento tecnológico e o controle do processo produtivo impulsionam a competitividade e se desenvolvem como fatores de segurança nacional. A energia nuclear, a nanotecnologia e as TICs são exemplos disso, visto que favorecem o sistema produtivo, o poder econômico, os recursos de força e o poder dissuasivo (MOREIRA, 2012).

Nesse sentido, a avaliação do poder cibernético dos países se torna um importante fator na compreensão das relações internacionais. Considerando o Estado como o principal ator tanto nas relações internacionais quanto no domínio cibernético, pode-se analisar o poder cibernético de uma nação a partir de três dimensões: “coordenação de operações e aspectos políticos nas estruturas governamentais; coerência de políticas através de alianças internacionais e doutrinas legais; e cooperação com atores cibernéticos não estatais” (KLIMBURG, 2011, p. 43, tradução nossa)[16]. Com isso, interpreta-se que a forma como os governos nacionais lidam com a questão do ciberespaço em relação à população de seus países e o sistema internacional, como a questão da livre circulação de informações e o fornecimento de serviços e recursos digitais, resulta direta ou indiretamente na dimensão do poder cibernético que o país possui (KLIMBURG, 2011).

Porém, apesar do poder cibernético ser cada vez mais um fator determinante nas relações de poder entre os Estados, o fácil acesso, a complicada delimitação territorial e a falta

[16] Texto original: coordination of operational and policy aspects across governamental structures, coherency of policy through international aliances and legal frameworks, and cooperation of non-state cyber actors

de uma governança global suscitam que o sistema internacional vive uma anarquia no plano cibernético, que segundo as ideias realistas podem gerar um dilema de defesa nacional e um estado de todos contra todos. Nesse sentido, a busca pela garantia do monopólio do uso da força pelo Estado seria inevitável, visto que o Estado possui como objetivo maior a sua sobrevivência nesse sistema. Assim, encontrar uma maneira de garantir essa legitimidade soberana em relação a um espaço invisível está sendo o maior desafio para os países.

As leis e o direito internacional surgiram anteriormente ao advento do ciberespaço, mas muitos argumentam que as mesmas previsões legais referentes à guerra tradicional podem ser totalmente aplicadas para ele (KHANNA, 2018). Há por outro lado, a visão de que um ataque cibernético é inerentemente distinto de um ataque físico que envolve o uso de instrumentos de guerra e, portanto, um novo sistema de regulação deve ser elaborado (KHANNA, 2018). Enquanto isso, até hoje somente a França, no ano de 2019, se pronunciou reconhecendo a soberania e a independência dos Estados no ciberespaço de acordo com a aplicabilidade do direito internacional atual (SCHMITT, 2019).

Apenas o Manual de Tallinn (2013), documento não oficial produzido por um grupo de especialistas internacionais patrocinados pelo Centro de Excelência em Defesa Cibernética da OTAN, elucida sobre o direito exclusivo que os Estados possuem de exercer sua jurisdição sobre infraestruturas cibernéticas e atividades que estão sobre o seu território. Contudo, o Manual não possui autoridade legal na comunidade internacional, serve apenas como uma espécie de recomendação já que não há uma convenção internacional oficial.

Isso posto, pensando em um exemplo hipotético, como determinar se informações enviadas por usuário de internet localizado na América do Sul, que compartilha um e-mail para outro usuário que se localiza na Europa, está rompendo com a soberania de todos os possíveis países envolvidos nesse fluxo de informação, visto que essas informações passam primeiro por servidores norte americanos para depois chegar a servidores europeus? Para o ciberespaço global atual, não há resposta objetiva para esse tipo de questionamento.

Dessa forma, temos que a anarquia do ciberespaço global é caracterizada pela falta de controle nas disputas de poder dentro desse espaço ao mesmo tempo em que o sistema internacional é caracterizado pelos interesses dos Estados soberanos. E esses Estados, conforme Alexander Wendt (1992), têm os seus cálculos afetados justamente pela distribuição de poder no sistema internacional.

Porém, segundo o autor, a forma como esses cálculos ocorrem dependem de uma compreensão intersubjetiva e das expectativas que possuem, assim como as concepções que constituem acerca de si próprio e dos outros. Com o argumento de que a "anarquia é o que os

Estados fazem dela" (WENDT, 1992, p. 395), o autor, juntamente com o movimento construtivista, possui a concepção de que o processo de formação de identidades e de interesses são endógenas as interações entre os atores, não sendo algo estritamente dado pela estrutura na qual está inserido. Ou seja, se a política internacional está fundamentada em um sistema de autoajuda no qual a obtenção da segurança é princípio vital para a sobrevivência de um ator, isso se deve ao processo e as ações conjuntas que construíram a estrutura e a situação em que se encontram.

A anarquia nesse caso possui apenas um papel de permissividade e a construção social é a responsável pela criação dos interesses e identidades que os seres humanos e, consequentemente, os Estados possuem. Com isso, um Estado pode ter múltiplas identidades. Assim como um indivíduo que possui diversas identidades a partir das suas funções e representações institucionais, o Estado as adquire por meio da interação coletiva com os demais atores no sistema internacional. Como resultado, seus interesses também serão fruto da forma como essas interações ocorrem e as identidades na qual cada Estado vai adotando sobre si e sobre os outros. "Os atores não tem um "portfólio" de interesses que carregam independentemente do contexto social; contrariamente, eles definem seus interesses no processo de definição das situações" (WENDT, 1992, p. 398).

O interesse próprio tem sido utilizado nas Relações Internacionais, especialmente pelos realistas, como o fator de justificativa para a maior parte das iniciativas e ações tomadas pelos países, seja em busca de poder, segurança, sobrevivência e/ou prosperidade. O conceito implícito nessa análise é de que os atores internacionais são racionais e tomam medidas apenas quando avaliam benefícios e efeitos positivos para si a partir delas. Wendt (1999) assume isso como realidade no sistema internacional, contudo, argumenta que essa visão de mundo é limitada e elimina a possibilidade dos Estados de se ajudarem mutuamente mesmo que suas seguranças não estejam diretamente ameaçadas, ou de que normas internacionais nunca seriam internalizadas e vistas como boas práticas a serem adotadas para uma melhor convivência entre a comunidade internacional.

Dessa forma, o dilema da segurança e a natureza insegura das nações, que gerariam um ambiente de competição e um sistema de soma zero, na visão realista, no qual o ganho de um corresponde a perda do outro, pode ser analisado como a construção de identidades negativas dos Estados em conjunto com interesses egoístas gerados a partir de concepções formuladas de maneira endógena, somado com as suas relações com outros atores.

A análise construtivista considera o Estado inicialmente como o produto de uma sociedade doméstica, que posteriormente traça a sua interação no processo constitutivo da

sociedade internacional. Assim sendo, a ação na política internacional depende das probabilidades que os Estados atribuem à determinada situação, sendo essa atribuição determinante para guiar ao conflito ou à cooperação. A soberania, por exemplo, somente existe pelo fato de que há o reconhecimento por parte de todos de que os Estados possuem o direito à propriedade territorial e a legitimidade do monopólio do uso da força.

Assim, a soberania pode ser definida como “[...] não apenas a liberdade de ação relativa à sociedade, ou a autonomia do Estado, mas sendo reconhecida pela sociedade como possuidora de certos poderes, tendo autoridade” (WENDT, 1999, p. 206-207, tradução nossa)[17]. Ou seja, sem o reconhecimento e a atribuição de identidades por si e pelos outros, a soberania não alcança o seu grau necessário de legitimidade

Trazendo o raciocínio para o contexto do ciberespaço, tem-se que a dificuldade de lidar com incidentes cibernéticos, devido à falta de clareza sobre o que constitui um ataque ou crime cibernético e a sua difícil atribuição, dado a complexidade dos atores envolvidos, faz com que estejamos ainda no processo de construção de identidades e interesses nesse espaço. Ou seja, espaço cibernético, além de invisível e imaterial, é novo e a sua exploração ainda está em fase inicial, de descobrimentos de suas capacidades.

Com isso, a difusão de poder propiciada pelo ciberespaço faz com que os Estados passem a modificar as suas concepções de identidade e de interesses. A securitização do espaço cibernético, por exemplo, pode ser vista como produto dessa modificação, que também pode alterar a forma como os países interagem no sistema internacional, visto que a ausência de regulamentação internacional para o ciberespaço atua de maneira permissiva para que a construção social da cooperação ou do conflito seja realizada.

No ambiente interno essas modificações já são realidade. Quando surgiu, o advento da internet e do ambiente virtual trouxe um pensamento libertário de que a informação teria sua circulação totalmente livre e que isso poderia representar um fim para o controle governamental. Entretanto, os governos continuaram exercendo sua soberania e formulando leis nacionais para adequar o uso do espaço cibernético conforme os direitos e deveres constitucionais de seus cidadãos, como questões de direitos autorais e propriedade intelectual.

Já no ambiente externo, o que existe é uma certa carência de uma governança no ciberespaço e Joseph Nye (2010) caracteriza isso como um “regime complexo”, onde há uma governança considerada imperfeita ou incompleta, visto que as diretrizes nacionais dos Estados prevalecem, bem como as suas interpretações e implementações. O regime complexo, portanto,

---

[17] Texto original: [...] is not about *de facto* freedom of action relative to Society, or “state autonomy”, but about being recognized by Society as having certain powers, as having authority.

seria configurado por "[...] instituições e normas livremente acopladas em algum lugar entre uma instituição integrada que impõem regulações através de regras hierarquizadas e instituições e práticas altamente fragmentadas sem um núcleo identificável e ligações não existentes" (NYE, 2010, p. 15, tradução nossa)[18].

Levando tudo isso em consideração, interpreta-se que, por ser emergente, a questão cibernética ainda está sendo construída e os interesses nesse espaço e as suas fronteiras, assim como as fronteiras políticas tradicionais, podem variar conforme o significado social que lhes for dado. Sendo assim, os documentos governamentais sobre defesa e segurança cibernética confeccionados principalmente por países de grande peso e influência regional e/ou mundial, como Estados Unidos, China e Israel, podem ser vistos como passos ou medidas para a construção de um significado social para o ciberespaço em âmbito internacional. Iniciando um processo de reconhecimento das ameaças, limites, vantagens e desvantagens, tanto externas quanto internas, que esse espaço representa. Por isso a importância da análise desses documentos.

Pois, assim como elucida Alexander Wendt em seu livro "*Social Theory of International Politics":*

> [...] Estados são efeitos de construções de barreiras assim como são suas causas. Além disso, a interação sistêmica é importante não apenas no início da determinação das barreiras, mas também na sua sustentação ao longo do tempo. Se as barreiras são estáveis, isso ocorre ou porque os Estados têm poder suficiente para evitar que outros os desafiem unilateralmente, ou porque eles reconhecem as fronteiras uns dos outros como legítimas. (WENDT, 1999, p. 213, tradução nossa)[19]

O Estado acaba sendo o maior interessado pela intensificação do controle do ciberespaço, visto que o seu gerenciamento afeta resultados nos demais domínios espaciais e em outros fatores da dimensão do poder. Pois, sendo responsável por enormes fluxos de informações, o espaço cibernético se estabelece como um facilitador da vida das pessoas, instituições e empresas. Com isso, os governos passaram a usufruir do ciberespaço para aprimorar a administração de suas infraestruturas estratégicas, como o funcionamento da rede de transportes, comunicação e do setor financeiro; para preservar e compartilhar informações consideradas confidenciais e de extrema importância para o funcionamento estável do país e

---

[18] Texto original: loosely coupled norms and institutions somewehere between and integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages.

[19] Texto original: [...] states are effects of boundary construction as much as they are its causes. Moreover, systemic interaction is importante not only in the initial determination of boundaries but in sustaining them over time. If boundaries are stable, this will either be because states have enough power to prevent others from changing them unilaterally, or because they recognize each other's border as legitimate.

para oferecer serviços importantes à população, como a geração e distribuição de energia, (FERREIRA, 2017).

Além disso, a utilização de TICs para ações ofensivas no ambiente cibernético, como no caso *Stuxnet* já comentado, passou a gerar preocupações para os Estados, no sentido de que o ciberespaço pode ser manuseado para a obtenção de interesses por meio de comportamentos hostis. Comportamentos estes que podem representar a ação de um adversário que almeja adquirir ganhos através dessas atividades, seja para conseguir informações, debilitar ou destruir o sistema de outro ator ou apenas impossibilitar o seu uso de modo legítimo (SINGER; FRIEDMAN, 2013).

Após compreender melhor sobre o ciberespaço e como ele pode impactar a visão e as ações dos Estados no âmbito da segurança internacional, podemos partir para a análise específica dos documentos governamentais de Estados Unidos, China e Israel, buscando entender as suas concepções sobre esse espaço e quais são as suas diretrizes de defesa e segurança cibernética.

3 AS ESTRATÉGIAS CIBERNÉTICAS NACIONAIS DE EUA, CHINA E ISRAEL

Neste capítulo serão analisadas as estratégias cibernéticas nacionais de Estados Unidos, China e Israel, a fim de compreender a forma como cada um aborda o tema e se é possível identificar tendências estratégicas a partir de convergências e divergências entre as suas visões. Conforme argumentado no capítulo anterior, a falta de convenções e normas internacionais a respeito do espaço cibernético cria um cenário de permissividade em que os governos nacionais decretam as suas próprias leis e regulamentos a partir do entendimento que possuem sobre esse novo domínio.

Consequentemente, as restrições de comportamentos dos Estados no ambiente cibernético surgem a partir das suas interações, dos regulamentos já existentes no direito internacional e dos mecanismos multilaterais sobre soberania, guerra e agressões. Dessa forma, surge a importância de analisar os documentos oficiais dos países sobre defesa e segurança cibernética, pois são as fontes primárias para entendermos como os Estados lidam com o ciberespaço. Muitos países demonstram se importar e destacar o setor cibernético como um importante fator para o desenvolvimento da nação e a estabilidade do país, tendo a digitalização de produtos e serviços muito presentes em suas sociedades. Como é o caso da Estônia, que figura na quinta posição mundial em segurança cibernética segundo o índice *Global Cybersecurity Index* 2018, relatório produzido pela UIT.

Entretanto, apesar de ser considerada uma sociedade digitalmente avançada, com a utilização do ciberespaço muito presente na vida dos cidadãos estonianos, não podemos considerar a Estônia como um relevante país na comunidade internacional, com grande influência e projeção de poder mundial. Com isso, a escolha por Estados Unidos, China e Israel foi baseada não apenas nas suas grandes capacidades cibernéticas, que segundo o mesmo índice aparecem na 2ª, 27ª e 39ª colocação global, respectivamente. Mas também pela grande notoriedade e influência que possuem na política internacional e regional.

Esse aspecto precisa ser levado em consideração já que a finalidade desta pesquisa é analisar se há indícios de que o peso das políticas de potências cibernéticas mundiais influi nas políticas cibernéticas de países periféricos como o Brasil. Sendo assim, este segundo capítulo possui a intenção de observar os pontos que se destacam nas estratégias cibernéticas nacionais dos três países citados e ponderar as suas aproximações e distanciamentos, de forma a conjecturar padrões e as suas compreensões políticas no que tange ao ciberespaço.

3.1 Estados Unidos

O estabelecimento de objetivos estratégicos em relação à segurança cibernética estadunidense foi introduzido no país em 2003, com a publicação do documento "Estratégia Nacional para Proteger o Ciberespaço"[20], pela Casa Branca, no qual deliberava as três principais metas a serem atingidas em âmbito nacional: "(i) prevenir ataques cibernéticos contra infraestruturas críticas, (ii) reduzir a vulnerabilidade nacional à ciberataques e (iii) minimizar os danos e prejuízos, aprimorando o tempo de resposta em relação a ocorrência de ataques no ciberespaço" (WHITE HOUSE, 2003, p. viii, tradução nossa)[21].

Após seis anos, em 2009, o governo estadunidense, sob o comando de Barack Obama, introduz as suas perspectivas e visões políticas sobre o ciberespaço. É publicado a "Revisão da Política para o Ciberespaço"[22], reconhecendo oficialmente o espaço cibernético como um ambiente passível de riscos e ameaças que podem afetar diretamente a economia e a segurança nacional. Esse reconhecimento levou em consideração que a sociedade estadunidense é cada vez mais dependente da internet para realizar as suas atividades e serviços diários básicos, representado no crescimento substancial do acesso à dispositivos de redes e redes de telecomunicação pela população (WHITE HOUSE, 2009).

O documento consiste em planos de ações políticas para serem tomadas, servindo como uma espécie de guia inicial para a segurança do país na "era cibernética". A compreensão estadunidense concluiu que havia a necessidade da formulação de uma estrutura política estratégica que garantisse, de forma coordenada, uma resposta do governo, do setor privado e dos seus aliados para a significativa ameaça cibernética (WHITE HOUSE, 2009). É a partir desse momento que a segurança cibernética passa a ter um papel de destaque nos assuntos de interesse nacional no país.

A publicação também compara o momento atual com o período vivido na Guerra Fria após o lançamento do satélite *Sputnik* em 1957, em que a corrida tecnológica global se acirrava e o país que obtivesse melhores resultados conseguiria estabelecer os seus interesses em âmbito mundial (WHITE HOUSE, 2009). O ciberespaço, portanto, é percebido pela Casa Branca como fator fundamental para que os EUA consigam atingir os seus objetivos econômicos, políticos e sociais e assegure o avanço das instituições democráticas, as liberdades civis e a segurança nacional.

[20] Texto original: National Strategy to Secure Cyberspace
[21] Texto original: (i) Prevent cyber attacks against America's critical infrastructure; (ii) Reduce national vulnerability to cyber attacks; and (iii) Minimize damage and recovery time from cyber attacks that do occur.
[22] Texto original: Cyberspace Policy Review

Por isso, o estabelecimento do diálogo e da aproximação entre sociedade, setor privado e academia em conjunto com o Estado para que um plano de ação efetivo seja posto em prática é visto no documento como essencial para que os Estados Unidos mantenham seu papel de líder internacional (WHITE HOUSE, 2009). Há o diagnóstico por parte do governo de que era preciso reforçar as instituições políticas e sociais no país, em um trabalho coordenado pelo governo federal e os seus principais departamentos para que a estratégia nacional elaborada se materializasse em ações práticas.

Com isso, não demorou muito para que o espaço cibernético emergisse como um domínio a ser securitizado. Em 2011, é promulgado o documento "Estratégia Militar Nacional dos Estados Unidos da América"[23], em que o ciberespaço é categorizado como um domínio de poder, se juntando aos domínios tradicionais: ar, terra, mar e espaço. A partir desse momento ocorre uma maior militarização do ciberespaço, pois declara-se que o seu aprimoramento pode resultar em um aumento da capacidade dos EUA em lutar guerras e na sua habilidade em atribuir e anular ataques em seus sistemas e infraestruturas (JOINT CHIEFS OF STAFF, 2011).

Essas infraestruturas são elencadas como infraestruturas críticas do país, consideradas vitais para a estabilidade social, econômica e política da nação, em vista das atribuições, funções, serviços e produtos que fornecem. Os Estados Unidos são cientes dos problemas e consequências negativas que o não funcionamento dessas infraestruturas podem causar. Por isso, produziu um plano de ação específico para garantir a proteção das suas infraestruturas críticas, o "Plano Nacional de Proteção a Infraestrutura"[24] (NIPP) (2013).

Nele, é atribuído ao *Department of Homeland State* (DHS) a responsabilidade de prevenir e responder à incidentes de segurança cibernética que afetem as infraestruturas críticas. Além disso, estabelece que deve haver o compartilhamento de informações a partir da parceria entre o DHS e o setor privado, que detém grande parte dessas infraestruturas. O documento define as infraestruturas críticas como:

> [...] sistemas e espólios, físicos ou virtuais, tão vitais para os Estados Unidos que as suas incapacidades ou destruição podem causar um impacto debilitante na segurança, na segurança econômica nacional, no sistema público nacional de saúde ou qualquer combinação nesses âmbitos (DEPARTMENT OF HOMELAND SECURITY, 2013, p. 7, tradução nossa)[25].

A justificativa do governo dos EUA para a elaboração do NIPP (2013) consiste no crescimento da interdependência entre os sistemas das infraestruturas críticas, principalmente

---

[23] Texto original: The National Military Strategy of the United States of America

[24] Texto original: National Infrastructure Protection Plan

[25] Texto original: [...] systems and assets, wheter physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

as baseadas em TICs, pois são mais vulneráveis às ameaças cibernéticas e a sua desestabilização pode resultar no comprometimento dos sistemas e redes interligados a ela. Segundo o documento, são consideradas infraestruturas críticas os setores:

> Químicos, facilidades comerciais, comunicação, manufaturados críticos, barragens, serviços de emergências, tecnologias da informação, materiais e reatores nucleares, agricultura e alimentos, base industrial de defesa, energia, saúde pública, serviços financeiros, sistemas de água, facilidades governamentais e os sistemas de transporte (DEPARTMENT OF HOMELAND SECURITY, p. 11, 2013, tradução nossa)[26].

Grande parte das infraestruturas críticas dos Estados Unidos são de controle do setor privado, sendo responsáveis pelo desenvolvimento dos equipamentos, recursos e capacidades das instalações. À vista disso, o governo esclarece no NIPP (2013) a responsabilidade do DHS em promover parcerias entre o setor público e o privado. A aproximação entre os dois setores é considerada crucial para que a proteção e a segurança das infraestruturas sejam garantidas. Nesse sentido, considera-se que o compartilhamento de informações entre as agências do governo federal e os operadores das infraestruturas críticas resulta em uma maior possibilidade de melhor entendimento sobre os riscos e vulnerabilidades, fazendo com que ambas as entidades responsáveis tomem decisões mais acuradas no que diz respeito à prevenção e defesa dessas infraestruturas (DEPARTMENT OF HOMELAND SECURITY, 2013).

O entendimento se baseia na interpretação de que em um mundo onde a confiabilidade de uma infraestrutura crítica é compartilhada entre a indústria e o governo, uma parceria sustentável deve ser construída e desenvolvida para que operações e atividades cibernéticas possam ser executadas (DEPARTMENT OF DEFENSE, 2018a). Contudo, a maneira pela qual essa interação ocorre na prática apresenta uma grande dificuldade de mensuração, visto que o governo dos EUA possui uma vasta e complicada burocracia, com grandes quantidades de agências, escritórios, conselhos, em escalas subdimensionais que respondem aos órgãos e departamentos de primeira ordem (PERNIK, 2016).

A população americana – em sintonia com o resto do mundo – vem se tornando cada vez mais dependente da internet para as suas conveniências e atividades diárias. O crescimento exponencial do acesso às redes de comunicação virtuais e a computadores possibilitou novas oportunidades e inovações no ramo tecnológico, mas esse grande nível de conectividade ao mesmo tempo introduziu progressivamente novos riscos e ameaças dentro do ambiente cibernético aos Estados Unidos (DEPARTMENT OF HOMELAND SECURITY, 2018). Esse

[26] Texto original: Chemical, commercial facilities, communications, critical manufacturing, dams, emergency services, information techonlogy, nuclear reactors, materials and waste, food & agriculture, defense industrial base, energy, healthcare & public health, financial services, water & wastewater systems, government facilitires, transportation systems.

entendimento está presente no documento "Estratégia de Segurança Cibernética do Departamento de Segurança Interna dos Estados Unidos"[27] (2018), em que o DHS decreta a previsão de que em 2023 a atividade cibernética ilícita irá declinar e um aprimoramento da segurança e da resiliência, bem como o fomento de um ecossistema cibernético confiável, irão ser implementadas no país.

Interpreta-se que a justificativa para essa estimativa se concentra em todos os esforços na implementação de medidas no setor cibernético em âmbito nacional nos últimos anos. Pois, é vital para os Estados Unidos que as suas lideranças governamentais estabeleçam e desenvolvam estratégias eficazes de proteção e recuperação para responder aos efeitos que dificultam o funcionamento normal da nação (DE LAURA, 2010). Dessa forma, são abordados no documento cincos pilares fundamentais em que os objetivos da estratégia de segurança cibernética se apoiam, são eles: (i) identificação de riscos, (ii) redução de vulnerabilidades, (iii) redução de ameaças, (iv) mitigação de consequências e (v) a habilitação de resultados de cibersegurança (DEPARTMENT OF HOMELAND SECURITY, 2018).

Além disso, nesse documento o DHS considera que o ecossistema do ciberespaço envolve não apenas as redes de tecnologias da informação e comunicação interconectadas, mas também tudo aquilo no qual o ciberespaço afeta e é afetado, como as pessoas, o meio ambiente, o aparelho legislativo e normativo da nação e condicionantes que influenciam as redes de comunicação e o funcionamento do espaço cibernético (DEPARTMENT OF HOMELAND SECURITY, 2018).

Desse modo, como forma de executar o pilar de identificação de riscos, é ressaltado mais uma vez a importância da boa relação entre o setor público e privado, bem como um bom ambiente internacional, em que políticas de cooperação em conjunto com os países aliados aos EUA devem ser feitas. Assim, o DHS fica incumbido de aumentar a consciência da nação sobre as possíveis ameaças, operando capacidades e oferecendo ferramentas e serviços que auxiliem a segurança cibernética das demais agências governamentais (DEPARTMENT OF HOMELAND SECURITY, 2018).

O pilar da mitigação de consequências também merece destaque, pois nele está embutido o conceito de resiliência. O intuito do governo estadunidense é minimizar as potenciais consequências de um ataque ou uma perturbação cibernética por meio de ações e respostas rápidas e coordenadas de toda a sociedade (DEPARTMENT OF HOMELAND SECURITY, 2018). Como visto no primeiro capítulo, o controle do número de ataques e

[27] Texto original: U.S Department of Homeland and Security Cybersecurity Strategy

ameaças e a total proteção das redes e sistemas ainda é algo inalcançável, devido às características do ciberespaço. Logo, ter a capacidade de reestabelecer o funcionamento normal de sistemas e equipamentos que sofreram incidentes em um menor tempo possível irá resultar na contenção de danos e prejuízos.

Segundo a “Estratégia de Segurança Nacional dos Estados Unidos da América”[28] (2017), a definição de resiliência consiste na “[...] habilidade de resistir e se recuperar de forma rápida de ataques deliberados, acidentes, desastres naturais, assim como estresses inconvencionais, choques e ameaças ao nosso sistema econômico e democrático” (WHITE HOUSE, 2017, p. 14, tradução nossa)[29]. Um dos métodos expostos no documento para a atenuação de consequências, ou resiliência cibernética, é incentivar o relato voluntário de incidentes e facilitar a notificação das vítimas de um ataque cibernético. O DHS, portanto, encoraja uma cultura de comunicação e compartilhamento de informações juntamente com uma cooperação efetiva entre as agências para aperfeiçoar o tempo de reação e as competências das respostas.

Em relação à habilitação de resultados no âmbito cibernético, último pilar citado, um dos seus objetivos se concentra na expansão da colaboração internacional em segurança cibernética para melhorar o ecossistema do ciberespaço. Esse tópico também é realçado em outros documentos oficiais do governo, como na “Estratégia Cibernética Nacional dos Estados Unidos da América”[30] (2018), em que o engajamento internacional sobre o assunto é dado como benéfico para as nações. Os Estados Unidos se comprometem a contribuir com mecanismos que favoreça uma coordenação internacional em defesa e segurança cibernética, fortalecendo parcerias que auxilie na proteção e investigação de crimes cibernéticos sem fronteiras, principalmente o ciberterrorismo internacional (WHITE HOUSE, 2018).

Essa cooperação internacional, de acordo com o governo estadunidense, deve ocorrer de modo estratégica, mediante alianças e parcerias julgadas como favoráveis aos interesses estadunidenses, garantindo que os valores americanos, como os princípios de uma internet livre sejam respeitados e mantidos (WHITE HOUSE, 2018). O âmbito internacional, portanto, é avaliado como um ambiente capaz de servir como ferramenta para a construção de melhores capacidades e práticas de defesa e segurança cibernética, tanto para os Estados Unidos quanto

[28] Texto original: National Security Strategy of the United States of America
[29] Texto original: [...] ability to withstand and recover rapidly from deliberate attacks, accidents, natural disasters, as well as unconventional stresses, shocks, and threats to our economy and democratic system.
[30] Texto original: National Cyber Strategy of the United States of America

para os seus parceiros, com o intuito de otimizar os seus recursos, infraestruturas críticas e fortalecer o ciberespaço por meio do compartilhamento de informações e ações mútuas.

Entretanto, os EUA deixam claro a sua intenção de permanecer como a liderança global e atuar de maneira que as outras nações assegurem publicamente que, ao formarem alianças na esfera da cibersegurança e ciberdefesa, irão seguir as concepções e os princípios estadunidenses (WHITE HOUSE, 2018). “Os Estados Unidos irão manter uma postura de ativa liderança internacional para avançar a influência americana e abordar um crescente conjunto de ameaças e desafios aos seus interesses no ciberespaço.” (WHITE HOUSE, 2018, p. 24, tradução nossa)[31]. O pretexto do governo se encontra no argumento de que, dessa forma, a colaboração entre os parceiros e aliados internacionais contribuirá para que a comunicação e o comércio transfronteiriço continuem garantidos no mundo, graças à arquitetura interoperável e aberta da internet (WHITE HOUSE, 2018).

A Organização do Tratado do Atlântico Norte (OTAN), por exemplo, pode ser vista como um instrumento de implementação dessa visão. Caracterizada por ser uma aliança militar intergovernamental baseada no sistema de defesa coletiva, a organização possui a sua própria política e estrutura de defesa cibernética, incentivada pelos seus países membros, sendo os EUA seu maior patrocinador (EFTHYMIOPOULOS, 2019). O progresso das inovações tecnológicas e das capacidades cibernéticas é considerado vital para o desenvolvimento das forças militares da OTAN e para a viabilidade de operações coordenadas entre os seus membros.

> Defesa inteligente e muito mais, na área da segurança cibernética, é a principal prioridade política da OTAN. No entanto, reflete também nas ferramentas e mecanismos usados na sua inovação e no gerenciamento de operações, processos e táticas. Permitindo o pensamento e a aplicação para o empresarial da defesa. (EFTHYMIOPOULOS, p. 11, 2019, tradução nossa)[32]

É interpretável, portanto, que os Estados Unidos se utilizem do setor cibernético para a projeção de seu poder na política internacional. No documento “Resumo da Estratégia Cibernética”[33] (2018), elaborado pelo *Department of Defense* (DoD), menciona-se que a Força Conjunta do Estado irá empregar capacidades cibernéticas ofensivas para realizar operações no ciberespaço por meio de todo o espectro de um conflito (DEPARTMENT OF DEFENSE, 2018a). De maneira assertiva, é elucidado que o país se utilizará da força para eliminar as suas ameaças e adversários, em um processo no qual o DoD se compromete em acelerar o

---

[31] Texto original: The United States will maintain an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in cyberspace.

[32] Texto original: Smart defense and more so in the field of cybersecurity is NATO’s main priority policy. It does however reflect as well on to the tools and mechanisms used to innovated in and for management operations, processes, and tactics. It allows for defense entrepreneurial thinking and application.

[33] Texto original: Cyber Strategy Summary

desenvolvimento das capacidades cibernéticas tanto para o combate quanto para conter atores cibernéticos maliciosos. “Primeiro, devemos garantir a capacidade do exército dos Estados Unidos em lutar e ganhar guerras em qualquer domínio, incluindo o ciberespaço” (DEPARTMENT OF DEFENSE, 2018a, p. 2, tradução nossa)[34].

Essa postura mais incisiva em relação ao emprego de capacidades cibernéticas em ambientes de combate e de guerra ganhou força na administração Obama e continuou se intensificando no país. Foi ainda em 2009 que o DoD criou o Comando Ciber dos Estados Unidos (USCYBERCOM) na busca pela centralização e elevação das capacidades cibernéticas (HEALEY, 2013 *apud* MACHADO, 2014). O Comando é responsável por planejar, coordenar e conduzir atividades defensivas e ofensivas no ciberespaço, dando suporte às forças armadas dos EUA em realizar operações de forma segura, bem como proteger os sistemas de comando e controle e a infraestrutura do ciberespaço (U.S ARMY WAR COLLEGE, 2011).

Apesar da valorização do uso do ciberespaço para ataques e defesas cibernéticas, os EUA não possuem uma conceituação definida e clara para guerra cibernética e, consequentemente, o entendimento sobre quando e como se aplicam normas legais em relação ao termo se torna subjetivo. Nem mesmo no principal documento de conceituação e definição de termos relacionados à defesa e à segurança nacional do país, o “Dicionário do Departamento de Defesa sobre Termos Militares e Associativos”[35] (2020), não há menção sobre guerra cibernética. A falta de definição é problemática quando, por exemplo, o Presidente tem que responder a um ataque cibernético e deve determinar se esse ataque se configura como um ataque armado ou não, justificando legítima defesa (KIRSCH, 2012). De qualquer maneira, os ataques cibernéticos são vistos pelo governo estadunidense como uma ameaça real, podendo causar danos ao território nacional.

Ainda em relação à projeção de poder, na Estratégia Cibernética Nacional dos Estados Unidos da América (2018) é declarado que o ciberespaço não será tratado como uma categoria de políticas ou atividades separadas dos outros elementos que compõem o poder nacional dos Estados Unidos. Ademais, o documento cita de maneira direta os países vistos como seus adversários no cenário da política internacional - Rússia, Irã, China e Coréia do Norte - acusando-os de utilizar o espaço cibernético como meio para ameaçar e desafiar os EUA e seus aliados (WHITE HOUSE, 2018). Nesse sentido, a proteção da democracia é ressaltada e o DoD reconhece que a era digital criou desafios à nação, principalmente com a utilização do

[34] Texto original: First, we must ensure the U.S military’s ability to fight and win wars in any domain, including cyberspace.
[35] Texto original: DoD Dictionary of Military and Associated Terms

ciberespaço por atores maliciosos e inimigos estadunidenses, que podem roubar tecnologias, perturbar o comércio e desafiar o processo democrático do país (DEPARTMENT OF DEFENSE, 2018a).

No que se refere à questão econômica, o comércio digital no país tem se tornado cada vez mais relevante para a economia nacional. O crescimento do denominado *e-commerce* ocorre de maneira a acelerar a substituição da atividade comercial física, sendo que, segundo a *US Census Bureau*, estatisticamente o comércio digital de manufaturados totalizou US$ 3,3 trilhões no ano de 2013, representando um aumento de 11,1% em relação ao ano de 2012 (PERNIK, 2016). O fortalecimento do ambiente cibernético nacional, por conseguinte, é tido como estratégico para a prosperidade econômica do país.

Com isso, a Estratégia Cibernética Nacional dos Estados Unidos da América (2018) apresenta o objetivo claro de fomentar o desenvolvimento tecnológico no país, sendo enfatizado a necessidade da agilidade em inovações das TICs em contrapartida a seus competidores. Para isso, é ponderado a indispensabilidade da aproximação entre três setores: o Estado, a academia e o setor privado. A consideração de que o ciberespaço é fator chave, um motor para o crescimento econômico e a prosperidade, fez com que a priorização de investimentos em um plano nacional de pesquisas e desenvolvimento de cibersegurança fosse estabelecido pelo governo (WHITE HOUSE, 2018).

O programa, intitulado de *National Critical Infraestructure Security and Resilience Research and Development Plan*, alinha os interesses e investimentos dos departamentos e agências federais com indústrias privadas e centros de pesquisa, de forma a aprimorar as tecnologias digitais nacionais, no intuito de manter os EUA como líder tecnológico global e ter maior efetividade no combate a eventualidades, criminosas ou não, no ambiente cibernético (WHITE HOUSE, 2018).

Nesse ponto, é dado importância para o fator humano, pois é interpretado que o aumento de consciência sobre o ciberespaço leva a tomada de decisões mais seguras e acertadas. Por isso, o DoD busca pela incorporação de uma cultura cibernética institucional, em que os indivíduos de todos os níveis dentro do departamento possam ter um conhecimento aceitável sobre o domínio cibernético, podendo aplicar esse conhecimento em suas funções diárias (DEPARTMENT OF DEFENSE, 2018a).

As autoridades ficam com a responsabilidade de ter uma compreensão quase que total sobre o assunto.

> “Líderes e sua equipe precisam ser fluentes em ciber para que possam entender totalmente as implicações em cibersegurança das suas decisões e estejam posicionados para identificar oportunidades para alavancar o domínio do ciberespaço

> para ganhar vantagens estratégicas, operacionais e táticas” (DEPARTMENT OF DEFENSE, 2018a, p. 5, tradução nossa)[36].

Na verdade, o governo dos Estados Unidos vê como estratégico o incentivo dessa cultura cibernética para toda a sociedade, especialmente no cultivo de novos talentos no ramo digital e na sustentação de uma força de trabalho na esfera cibernética no país. O raciocínio é de que toda pessoa, incluindo os setores governamentais, privados e públicos, que usam um sistema de computador ou dispositivo de comunicação que possua internet, deve se conscientizar das ameaças e vulnerabilidades que o uso dessas tecnologias pode afetar em sua vida (DE LAURA, 2010).

Por conseguinte, o DoD fica encarregado por investir em futuros talentos e profissionais especializados, identificando e recrutando essas pessoas para trabalharem para o governo em prol dos interesses da nação. São delineadas tanto carreiras militares quantos civis no setor, permitindo processos de rotações entre os departamentos, agências e cadeias de comando, de forma a otimizar os serviços prestados e aperfeiçoar essa força de trabalho (DEPARTMENT OF DEFENSE, 2018a). Para atingir essa cultura cibernética, o poder público tem papel essencial na construção de uma estrutura educacional e informativa em toda a nação, promovendo, investindo e desenvolvendo disciplinas de ciência, tecnologia, engenharia, matemática e língua estrangeira em todo o nível primário e secundário de educação no território estadunidense (DEPARTMENT OF DEFENSE, 2018a).

O programa dirigente no aspecto educacional da nação é intitulado de *National Initiative for Cybersecurity Education* (NICE), possuindo como método o reforço da parceria entre a academia, o setor privado e o Estado, para que atuem de modo coordenado no treinamento e na educação dos profissionais da área cibernética (WHITE HOUSE, 2018). Tem-se o entendimento de que isso construirá uma sociedade com maior consciência sobre o ciberespaço e consequentemente o setor cibernético nacional será mais confiável e seguro.

Interpreta-se ainda, que há uma busca por padrões de comportamentos, do Estado e também da sociedade civil, que colaborem para que o objetivo primeiro, da prosperidade do modo de vida americano, seja garantido. “Como os Estados Unidos continuam a promover consenso no que constitui o comportamento estatal responsável no ciberespaço, nós também devemos trabalhar para garantir que haja consequências para comportamentos irresponsáveis

---

[36] Texto original: Leaders and their staffs needs to be “cyber fluent” so they can fully undertand the cybersecurity implications of their decisions and are positioned to identify opportunities to leverage the cyberspace domain to gain strategic, operational and tactical advantages.

que prejudiquem os Estados Unidos e seus aliados*"* (WHITE HOUSE, 2018, p. 21, tradução nossa)[37].

Em termos específicos de defesa nacional, o "Resumo da Estratégia de Defesa Nacional dos Estados Unidos da América"[38] (2018), constata o complexo cenário da segurança global, em que desafios são postos a uma ordem internacional aberta e livre, marcada pela competição entre as nações no mundo. Mais uma vez, o avanço das tecnologias é apontado como fator capaz de moldar o que hoje se entende a guerra. Entre essas tecnologias, é citado a inteligência artificial, computadores, a autonomia, robôs, energia direcionada, hipersônicos e a biotecnologia. (DEPARTMENT OF DEFENSE, 2018b). Por conseguinte, o documento preza pelo investimento em ciberdefesa, resiliência e integração das capacidades cibernéticas em todo o espectro das operações militares.

Ademais, o documento "Estratégia Nacional de Inteligência dos Estados Unidos da América"[39] (2019) examina que a abundância de dados e informações na qual o mundo possui atualmente dificulta o trabalho da comunidade da inteligência em coletar, processar, avaliar e analisar esse grande volume de dados e informações. Desse modo, os ataques cibernéticos, que podem ser o roubo de informações confidenciais ou a queda de sistemas de informação no país, são reconhecidos como uma ameaça direta à defesa nacional e o setor de inteligência nacional dos EUA é concebido como estratégico na preservação das capacidades cibernéticas do país e de um ciberespaço seguro (INTELLIGENCE COMMUNITY, 2019). No documento, a estratégia estabelecida pelo setor de inteligência dos Estados Unidos é de aprimorar a detecção das ameaças cibernéticas, identificando as informações que podem ser danosas aos país.

Com isso, uma inteligência de ameaças cibernéticas é instituída, com o objetivo de ter a capacidade de reconhecer as intenções dos atores estatais e não estatais estrangeiros, os seus programas cibernéticos, as suas capacidades, táticas operacionais, técnicas, atividades e indicadores que podem ter impactos diretos na segurança nacional dos EUA (INTELLIGENCE COMMUNITY, 2019). Para alcançar tal finalidade, a comunidade da inteligência do país se compromete a melhorar o seu entendimento sobre a utilização do ciberespaço pelos adversários do país. Decide, portanto, expandir a produção e divulgação de relatórios para apoiar a defesa das redes vitais de informações e as infraestruturas críticas e, por fim, abranger a possibilidade de planos e operações diplomáticas, militares, econômicas, financeiras, de inteligência e

[37] Texto original: As the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners.
[38] Texto original: Summary of the National Defense Strategy of the United States of America
[39] Texto original: National Intelligence Strategy of the United States of America

legislativas para conter atores e atividades cibernéticas maliciosas (INTELLIGENCE COMMUNITY, 2019).

3.2 China

Foi também em 2003 que a República Popular da China publicou seu primeiro documento oficial no que concerne à segurança cibernética no país. Denominado de "Pareceres do Grupo de Liderança Nacional em Informatização sobre Fortalecimento da Segurança da Informação"[40] (2003), é o início do entendimento do governo chinês, liderado por Xi Jinping, sobre o espaço cibernético e os possíveis desdobramentos das tecnologias da informação e comunicação no país. A terminologia utilizada pela China para o ciberespaço e segurança e defesa cibernética diverge em relação aos países ocidentais. Desde essa publicação, o país utiliza as expressões 'espaço da informação' ou 'espaço da rede' e 'segurança da informação' ou 'segurança da rede', para tratar sobre o assunto, ainda que hoje se encontre a palavra *cyber* em alguns textos ou pronunciamentos oficiais, os termos originais ainda ecoam na compreensão chinesa.

De forma sucinta, o documento declara que o rápido desenvolvimento da ciência e das tecnologias, como a internet, juntamente com a grande aceleração da economia chinesa e do processo de informatização da sua sociedade, fez com que a segurança da informação passasse ser vista como um fator para a garantia da segurança nacional. Com isso, melhorar o sistema cibernético defensivo é colocado como uma meta a ser atingida pelo país, por meio do desenvolvimento das capacidades de segurança da informação, construindo um saudável ambiente das redes e sistemas de informações. A instabilidade e a perturbação que ataques e crimes cibernéticos podem afetar na nação é destacado, pois há o reconhecimento de que, no período, a China carecia de regulamentos e leis fortes sobre segurança cibernética, de uma consciência total da sociedade sobre o assunto e de competitividade para a sua indústria nacional nesse setor (CHINA, 2003).

A militarização do assunto se intensificou no país apenas em 2014, com a divulgação do "Pareceres da Comissão Militar Central solicitando maior fortalecimento da Segurança Militar da Informação"[41] (2014), em que é apontado a necessidade do entendimento de que

[40] Texto original: **国家信息化**领导小组关于加强信息安全保障工作的意见.

[41] Texto original: **中央**军委印发《意见》要求进一步加强军队信息安全工作.

reforçar a segurança cibernética é um requisito inevitável para a nação evoluir na era da informação e uma tarefa urgente para se vencer guerras. É proposto que o nível de proteção e avaliação de riscos no setor cibernético deve ser elevado, construído e aplicado de maneira doméstica, consolidando a segurança da informação no país e inovando tecnologias e sistemas que sejam efetivos contra as ameaças ao espaço cibernético (CYBERSPACE ADMINISTRATION OF CHINA, 2014).

A intenção expressa nesse documento consiste em preparar e sofisticar as Forças Armadas da China para esse novo ambiente de guerra, para que tenham capacidades e recursos necessários para realizar suas tarefas, missões e operações de modo seguro e eficaz, tanto no presente quanto no futuro. Por isso, é recomendado a implementação de uma série de fatores no setor militar, como a divisão de responsabilidades entre as cadeias de comando, projetos coordenados, controle de riscos, promoção do gerenciamento centralizado da segurança cibernética e a aceleração do estabelecimento de uma proteção concreta para os sistemas e redes de informação nacionais, que vão de encontro com as necessidades militares do país (CYBERSPACE ADMINISTRATION OF CHINA, 2014).

A progressão sobre a importância do assunto para o governo chinês é notada com a determinação de diretrizes e estratégias para a segurança cibernética em âmbito nacional e internacional anos mais tarde. Isso ocorre com a promulgação da "Lei de Segurança Cibernética da República Popular da China"[42] (2016), sendo até hoje o principal documento do país em relação à sua visão política, econômica e social sobre o tema. O governo anuncia que a lei nasce com o propósito de salvaguardar a segurança das redes de informação, a soberania do ciberespaço, a segurança nacional, o interesse social, os direitos e deveres dos cidadãos e das organizações e promover o desenvolvimento saudável de uma sociedade da informação (OFFICE OF THE CENTRAL CYBERSPACE AFFAIRS COMMISSION, 2016).

O gerenciamento, coordenação e supervisão das medidas de segurança da informação tomadas no país ficam a cargo do poder público, representado pelo Estado e seus principais departamentos e agências. Há uma maior centralização em relação à autoridade, responsabilidade e funções no país, pois além de formular a estratégia nacional e estabelecer os objetivos, o Estado também possui a capacidade de adotar as medidas que considera necessárias e determina a subordinação de todos os setores ao poder público. Os operadores de rede no país, por exemplo, ficam submetidos a cumprir os regulamentos, disposições e leis deliberadas pelo governo, assumindo responsabilidades sociais e obrigações que concernem à segurança

[42] Texto original: 中华人民共和国网络安全法.

cibernética, aceitando a supervisão governamental (OFFICE OF THE CENTRAL CYBERSPACE AFFAIRS COMMISSION, 2016).

A lei também prevê que indivíduos e organizações que utilizam a internet devem seguir e respeitar as leis nacionais referentes ao setor cibernético, sendo incumbidos de não disseminar informações que podem colocar a segurança, a honra e os interesses nacionais em perigo, bem como a soberania da China e o seu sistema político (OFFICE OF THE CENTRAL CYBERSPACE AFFAIRS COMMISSION, 2016). A fabricação e a divulgação de informações falsas e danosas são vistas pelo governo chinês como uma ameaça à ordem econômica e social da nação, podendo infringir a reputação, a privacidade e os direitos legítimos de cada cidadão chinês. No mesmo sentido, o documento elucida que essas informações podem contribuir para a promoção do ódio contra a nação, do terrorismo, do extremismo, da discriminação étnica e da violência, podendo acarretar na destruição da unidade nacional (OFFICE OF THE CENTRAL CYBERSPACE AFFAIRS COMMISSION, 2016).

Porém, mesmo com a autoridade central do Estado, é ponderado como essencial uma relação de parceria entre o setor público e privado, que representa parte das indústrias de TICs e dos operadores e provedores de redes e serviços de telecomunicação no país. A cooperação e a colaboração entre os setores, portanto, funciona de maneira estratégica, em que o Estado serve como um guia para os procedimentos adotados pelas indústrias e operadores, possuindo o direito de supervisão e monitoramento determinado por lei. "Os operadores de rede devem cooperar com a supervisão e a inspeção do departamento de informações de rede e departamentos relevantes de acordo com a lei" (OFFICE OF THE CENTRAL CYBERSPACE AFFAIRS COMMISSION, 2016, p. 7, tradução nossa)[43].

Em relação aos riscos e ameaças cibernéticas, fica determinado que, caso causem algum incidente cibernético em nível nacional, serão confrontados com um plano de emergência que irá categorizar o grau dessa ameaça e estipular as respostas que devem ser dadas pelos atores. De maneira geral, a lei de 2016 elenca três principais medidas que devem ser tomadas caso haja chance de ocorrer um acidente cibernético, malicioso ou não:

> (i) realizar a coleta rápida de informações relevantes e reforçar o monitoramento dos riscos da segurança das redes; (ii) organizar os departamentos, agências e profissionais para analisar e avaliar as informações sobre os riscos de segurança cibernética, de modo à predizer e mensurar o escopo e a extensão do incidente; (iii) emitir avisos sobre os riscos cibernéticos para a sociedade e tomar medidas para a

[43] Texto original: 网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合.

> mitigação de danos (OFFICE OF THE CENTRAL CYBERSPACE AFFAIRS COMMISSION, 2016, p. 8, tradução nossa)[44].

Com uma abordagem semelhante à dos EUA, o governo chinês afirma que o uso e a disseminação em massa de informações e de tecnologias relacionadas a elas possuem um grande impacto no crescimento econômico e no progresso social, configurando a segurança cibernética como elementar para a paz mundial. Esse entendimento é reforçado no documento "Estratégia Nacional para a Segurança no Ciberespaço"[45] (2016), em que se traça a estratégia nacional da China em relação ao ciberespaço, com o intuito de construir uma sociedade próspera. Uma sociedade que seja capaz de utilizar o setor cibernético para a promoção de sua cultura, enriquecendo a vida de seus cidadãos culturalmente com a popularização do conhecimento, possibilitada pelos novos meios virtuais de propagação de informações (CYBERSPACE ADMINISTRATION OF CHINA, 2016).

Na visão chinesa, isso ocorre em vista do ciberespaço ser um novo espaço para a produção e para a vida. Admite-se que a intensidade da integração entre as redes, sistemas e a vida das pessoas, em aspectos como a forma de trabalhar, educação, comércio, finanças, assistência médica, entre outros, é tão forte que vem moldando a humanidade (CYBERSPACE ADMINISTRATION OF CHINA, 2016). Consequentemente, o ambiente cibernético é referido como um novo propulsor para o desenvolvimento econômico do país, especialmente através da transformação e da inovação das TICs. Nesse sentido, o fomento às indústrias nacionais é ponderado como estratégico, pois permite o aprimoramento dessas tecnologias e possibilita o desenvolvimento socioeconômico da China. "Sem segurança cibernética, não há segurança nacional. Sem informatização, não haverá modernização" (CYBERSPACE ADMINISTRATION OF CHINA, 2016, p. 4, tradução nossa)[46].

Além disso, o governo chinês enxerga o ciberespaço como uma nova plataforma para a governança. O ambiente virtual permitiu uma modernização no sistema de governo nacional, devido a facilitação da divulgação e compartilhamento de informações, estimulando tomadas de decisões científicas e populares pelo governo, visto que o espaço virtual serve como um canal para os cidadãos possuírem maior participação na governança social no país (CYBERSPACE ADMINISTRATION OF CHINA, 2016). O documento também esclarece

---

[44] Texto original: (i) **要求有关部**门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测; (ii) 组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度; (iii) 向社会发布网络安全风险预警，发布避免、减轻危害的措施.

[45] Texto original: **国家网**络空间安全战略.

[46] Texto original: **没有网**络安全就没有国家安全，没有信息化就没有现代化.

que a China considera o ciberespaço como um novo território para a soberania nacional, tão importante quanto os outros domínios tradicionais, fazendo com que a defesa e a segurança cibernética sejam elementos cruciais na manutenção e garantia da soberania pelo Estado.

"O governo chinês acredita que a internet é uma infraestrutura crítica da nação, que pertence ao território da República Popular da China, logo, está sob a jurisdição do país e, portanto, a soberania da internet chinesa deve ser respeitada e protegida" (CUIHONG, 2015, p. 6, tradução nossa)[47]. Conciliar a integração da comunidade internacional no ciberespaço com a não interferência externa, respeitando o direito de cada país em poder lidar com o espaço cibernético em âmbito nacional, pode ser visto como um objetivo da China. O governo chinês, contudo, apesar de trazer à tona e enfatizar o termo soberania da internet, não oferece uma definição consistente e clara sobre o que essa soberania representa e implica (ZENG et al., 2017). Apesar disso, é expressado na Estratégia Nacional de Segurança do Ciberespaço (2016) a pretensão da territorialização do ciberespaço, com o respeito pela soberania elencado como um dos principais princípios da estratégia chinesa.

No contexto chinês, defender essas fronteiras da informação significa que o governo precisa ativamente resistir à invasão de informações e ideias ocidentais, que podem colocar em xeque o sistema uni partidário vigente. (ZENG et al., 2017). O respeito por essa soberania é exposto no documento estratégico, portanto, como um meio para assegurar o direito de os países poderem decidir seus próprios caminhos de desenvolvimento cibernético, em relação às suas políticas públicas para o uso da internet e de poderem ter uma participação mais igualitária nos fóruns e organizações internacionais a respeito da governança internacional do ciberespaço (CYBERSPACE ADMINISTRATION OF CHINA, 2016).

É levado em consideração que os países possuem diferentes condições nacionais e experiências internacionais, sendo que precisam tomar as ações e medidas necessárias para gerenciar os seus sistemas e redes de informação dentro de seus territórios (CYBERSPACE ADMINISTRATION OF CHINA, 2016). Logo, interpreta-se que, pela visão chinesa, a transgressão da soberania nacional no espaço cibernético pode levar o país a uma maior exposição a interferências, perturbações, invasões e ataques cibernéticos que podem lesar a segurança e os interesses nacionais.

---

[47] Texto original: The Chinese government believes that the Internet belongs to critical national infrastructure, that Internet within the territory of the People's Republic of China is under the jurisdiction of Chinese sovereignty, and that China's Internet sovereignty shall be respect and protected

Com uma abordagem semelhante, o documento “Estratégia Internacional de Cooperação no Ciberespaço”[48] (2017), expressa que todos os países deveriam acatar a Carta das Nações Unidas, seguindo os princípios de não se utilizar da força, a fim de que o ciberespaço não gere uma corrida por armamentos cibernéticos entre os países. É manifestado que os países devem evitar a mentalidade de Guerra Fria, no qual persiste um jogo de soma zero que condiciona os comportamentos dos Estados, bem como que nenhum país persiga a hegemonia cibernética (MINISTRY OF FOREIGN AFFAIRS, 2017). O intuito é prevenir que as tecnologias sejam usadas para propósitos de conflitos, que não contribuem para a manutenção da estabilidade e da segurança internacional (MINISTRY OF FOREIGN AFFAIRS, 2017).

Em relação ao estabelecimento de uma governança global da internet, a China declara que a ONU deveria ser responsável por tutelar uma governança internacional, propiciando a internacionalização dos recursos de gerenciamento dos endereços e raízes dos servidores da internet. Enfatiza-se o princípio da busca e da luta por um mundo pacífico, em que a República Popular da China se compromete em trabalhar pela justiça e pela amizade entre os povos, tentando atingir uma cooperação *win-win* (MINISTRY OF FOREIGN AFFAIRS, 2017). Desse modo, a governança global do ciberespaço, na concepção chinesa, deve seguir uma abordagem multilateral e democrática, com grande participação de atores estatais e não estatais, como as companhias de internet, ONGs e indivíduos.

> Como uma nova fronteira, o ciberespaço precisa ser governado por regras e normas de comportamento. A China apoia a formulação de regras e normas internacionais universalmente aceitas de comportamento do Estado no ciberespaço, no âmbito das Nações Unidas, que estabelecerão princípios básicos para os Estados e outros atores para regular seus comportamentos e intensificar a cooperação, com a finalidade de manter a segurança, a estabilidade e a prosperidade no espaço cibernético (MINISTRY OF FOREIGN AFFAIRS, 2017, p. 5, tradução nossa)[49].

Há também a declarada intenção do governo chinês em reformar a ICANN, responsável pelos protocolos de endereços da internet, tornando-a em uma instituição internacional verdadeiramente independente, aumentando a sua representação e a transparência de suas decisões, para que os recursos, raízes e servidores da internet sejam distribuídos e gerenciados de maneira mais justa (MINISTRY OF FOREIGN AFFAIRS, 2017).

---

[48] Texto original: 网络空间国际合作战略.

[49] Texto original: 网络空间作为新疆域，亟需制定相关规则和行为规范. 中国主张在联合国框架下制定各国普遍接受的网络空间国际规则和国家行为规范，确立国家及各行为体在网络空间应遵循的基本准则，规范各方行为，促进各国合作，以维护网络空间的安全、稳定与繁.中国支持并积极参与国际规则制定进程，并将继续与国际社会加强对话合作，作出自己的贡献.

Ainda no mesmo documento, a China se mostra propensa à cooperação internacional no âmbito do ciberespaço, elucidando que a internet proporcionou um grande fluxo de informações ao redor do globo, interconectando e aproximando as civilizações do mundo. De modo benéfico, a aproximação é percebida como um reforço na difusão de tecnologias da internet para regiões periféricas e menos desenvolvidas, assim como possibilita o compartilhamento e o desenvolvimento conjunto de tecnologias que auxiliem no combate ao crime cibernético, práticas maliciosas e ciberterrorismo (MINISTRY OF FOREIGN AFFAIRS, 2017).

A preferência da República Popular da China pela ONU para liderar a governança global da internet pode ser vista como uma tentativa do país em ganhar capacidade de decisão e representatividade no gerenciamento do ciberespaço. O sistema da ONU permite que individualmente, Estados-nação tenham maior poder, devido ao peso de seus votos, do que em organizações que concedem diferentes sistemas de eleições, com diferentes pesos para os membros. Além disso, a China é membro permanente e teria maior influência para defender a sua ideia de internet soberana (SHEN, 2016).

A Estratégia Internacional de Cooperação no Ciberespaço (2017) também menciona que a ausência de leis e regulamentos internacionais para o ciberespaço, que governe de maneira efetiva o comportamento dos atores, contribui para dificultar o desenvolvimento do espaço virtual. Contudo, mais uma vez é reiterado a questão da soberania no espaço cibernético, de modo a almejar que normas e convenções internacionais garantam que os governos nacionais tenham o direito e a responsabilidade de administrar o espaço cibernético, estabelecendo a sua segurança em seu território sem interferências externas. De maneira convergente, a Estratégia Nacional para a Segurança no Ciberespaço (2016) declara que a China irá se opor a todos os atos que subverta o poder político do Estado chinês e debilite a sua soberania nacional por meio da internet (CYBERSPACE ADMINISTRATION OF CHINA, 2016).

Sendo assim, a estratégia cibernética internacional chinesa é continuar tendo uma participação ativa em fóruns e organizações multilaterais, propagando os valores da cultura chinesa, promovendo o desenvolvimento da economia digital global, do aprendizado mútuo e encorajando o comércio virtual ao mesmo tempo em que preserva a soberania e os seus interesses (MINISTRY OF FOREIGN AFFAIRS, 2017). É destacado, na Estratégia Internacional de Cooperação no Ciberespaço (2017), os empenhos feitos até então pelo país na comunidade internacional, como a submissão da proposta do Código de Conduta Internacional para a Segurança da Informação por meio da *Shanghai Cooperation Organization* (SCO) em

que se previa normas de comportamento para os Estados no ciberespaço. A proposta foi negada pelos EUA.

Outro ponto enfatizado tanto na Lei de 2016 quanto na Estratégia Nacional, do mesmo ano, é a proteção e o aperfeiçoamento das infraestruturas críticas do país. O governo se refere a elas como facilidades relacionadas à segurança nacional, economia e à subsistência da população. É enxergado que segurança cibernética nacional precisa ser robusta e resiliente para não colocar em risco as redes importantes de sistemas de informação, em que sua destruição ou mal funcionamento podem resultar sérios danos ao interesse público (CYBERSPACE ADMINISTRATION OF CHINA, 2016). São citados como infraestruturas críticas os sistemas de "energia, finanças, transportes, educação, pesquisa científica, conservatórios de água, manufatura industrial, assistência médica e de saúde, segurança social, serviços públicos, agências estatais e importantes sistemas da internet" (CYBERSPACE ADMINISTRATION OF CHINA, 2016, p. 2, tradução nossa)[50].

A defesa e proteção desses sistemas vitais fica a cargo do governo, das indústrias e da sociedade como um todo, sendo que as autoridades competentes possuem a função de orquestrar as unidades de operação e deve tomar as medidas necessárias para assegurar a segurança dos dados e das informações que fluem nas infraestruturas. O método admitido é reforçar a avaliação de riscos de informações chaves, a segurança dos órgãos governamentais; construir e operar um website base para as agências do governo em um modo intensivo e estabelecer mecanismos de compartilhamento de informações entre o governo e as empresas, dando suporte total para as empresas e indústrias em executar o seu papel de defender as infraestruturas críticas (CYBERSPACE ADMINISTRATION OF CHINA, 2016).

Os operadores das infraestruturas críticas recebem obrigações legais para manterem o funcionamento estável das infraestruturas. Uma vez identificado como parte de uma infraestrutura crítica do país, o operador de rede responsável será cobrado com mais obrigações onerosas de segurança cibernética que um operador de rede normal (QI et al. 2018). Alguns artigos da Lei de Segurança Cibernética da República Popular da China (2016) são dedicados a explicitar esses deveres, entre eles o planejamento, adoção e uso de medidas de segurança; treinamento e educação dos funcionários sobre segurança cibernética; cumprimento dos requisitos de confidencialidade para aquisição de produtos e serviços de rede e a realização de uma avaliação de segurança para a transferência de dados para o exterior.

---

[50] Texto original: **能源、交通、通信、金融等基**础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。

Em concordância com uma lógica de mercado e com o anseio pelo desenvolvimento econômico da China, os dois principais documentos estratégicos também registram a relevância do incremento de novas tecnologias para fortalecer a segurança cibernética. O papel do Estado é posto como central, determinando o direcionamento dos investimentos no setor cibernético para as empresas, instituições de pesquisa e ensino e organizações relacionadas às redes de informação e comunicação no país. O apoio do setor público, portanto, é vital para o funcionamento e o desenvolvimento dessas instituições e, consequentemente, das tecnologias pesquisadas, produzidas e fornecidas por elas. "O Estado apoia o gerenciamento inovador de segurança da rede e utiliza novas tecnologias de rede para aprimorar o nível de proteção de segurança da rede" (OFFICE OF THE CENTRAL CYBERSPACE AFFAIRS COMMISSION, 2016, p. 3, tradução nossa)[51].

Nas últimas três décadas o apoio estatal na inovação de tecnologias da informação foi posto em prática no país para operacionalizar a prioridade de modernizar e profissionalizar as Forças Armadas da nação, conduzir operações, controlar discursos na internet para manter a estabilidade política e assegurar as relações bilaterais e multilaterais no setor cibernético. (CHANG, 2014). O foco nas TICs e tecnologias de segurança cibernética, portanto, pode ser interpretado como um projeto de longa data do governo chinês, que tem como meta o desenvolvimento do país e a manutenção da segurança nacional.

Na Estratégia Nacional para a Segurança no Ciberespaço (2016), por exemplo, é tido como estratégico a implementação de iniciativas que acelerem o aperfeiçoamento da segurança dos softwares nacionais e de redes que enriquecem o ciberespaço nacional de informações confiáveis, com o intuito de revigorar a internet e estabelecer um sistema de gerenciamento de dados seguro. Dessa forma, o fomento das TICs de nova geração tem como objetivo conseguir aplicar, gerir e utilizar o *big data* e a computação em nuvem de maneira otimizada, melhorando o ambiente informacional e consolidando a base industrial para preservar a segurança cibernética do país (CYBERSPACE ADMINISTRATION OF CHINA, 2016).

Para esse fim, o capital humano é levado em consideração. A República Popular da China prevê um projeto para encontrar e incentivar talentos na área cibernética, construindo disciplinas e faculdades sobre cibersegurança, formando um ambiente sustentável na condução e cultivo de novos talentos, empreendedorismo e inovação (CYBERSPACE ADMINISTRATION OF CHINA, 2016). Também é proferido que estímulos serão feitos na educação fundamental, em métodos de ensino e recursos que possibilitem a melhora da literacia

[51] Texto original: 国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平.

da sociedade sobre o ciberespaço e segurança cibernética, elevando a consciência da população sobre o assunto (CYBERSPACE ADMINISTRATION OF CHINA, 2016). A expectativa é de que os usuários chineses da internet tenham suas habilidades cibernética melhoradas, aumentando sua capacidade de identificação e resiliência sobre crimes cibernéticos, fraudes online, ataques cibernéticos e atividades maliciosas no ciberespaço em geral.

A Lei de Segurança Cibernética da República Popular da China (2016) ainda dedica o seu capítulo final para decretar multas e responsabilidades legais que os operadores de rede e os indivíduos estão sujeitos caso não cumpram ou violem os artigos expostos em todo o documento. Os departamentos governamentais encarregados de monitorar e supervisionar os atores cibernéticos e os fluxos de informações no país possuem autoridade para aplicar penas monetárias a todos aqueles que fugirem de suas obrigações ou falharem em suas atividades, performance e funções, podendo colocar em risco à segurança nacional da China. Os valores das multas variam entre 5,000 e 500,000 yuans.

O modelo cibernético chinês também conta com outros regulamentos oficiais na esfera informacional. Publicados no mesmo ano, o "Regulamentos sobre a Proteção do Direito de Comunicação na Rede de Informações"[52] (2017) e o "Regulamentos sobre o Gerenciamento de Serviços Comerciais de acesso à Internet"[53] (2017) dizem respeito à proteção dos direitos autorais de organizações e indivíduos que realizam trabalhos, performances, produtos audiovisuais, serviços e outras atividades relacionadas ao âmbito da informação e da internet. No primeiro documento, é previsto dispositivos que garantem os direitos, deveres e responsabilidades dos provedores e clientes de produtos e serviços de informação, ficando expostos a punições em caso de não cumprimento ou violação dos artigos apresentados.

O segundo documento delibera sobre o uso e acesso público da internet por serviços comerciais, para que a segurança dos usuários e dos fornecedores de serviços online, como estabelecimentos de *cyber café* seja garantida. Os artigos preveem obrigações e deveres, sendo estabelecido tanto regras para o consumo dos serviços quanto para a sua oferta. Fica enfatizado os direitos à privacidade de dados e informações, com o Estado como o supervisor das atividades, estabelecendo multas e penas em caso de violação dos artigos promulgados (MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY, 2017b).

Outro regulamento nacional que tange a esfera cibernética é denominado de "Disposições sobre Supervisão e Inspeção de Segurança na Internet por Órgãos de Segurança

---

[52] Texto original: 信息网络传播权保护条例

[53] Texto original: 互联网上网服务营业场所管理条例

Pública"[54] (2018) e delineia regulamentações para as agências e órgãos estatais nas suas tarefas de inspecionar e supervisionar a segurança da internet. O objetivo é que as medidas contribuam para prevenir crimes cibernéticos, de forma a resguardar a segurança cibernética e proteger os legítimos direitos e interesses dos cidadãos, pessoas legais e organizações. A inspeção e a supervisão podem acontecer de maneira remota e os provedores e usuários da internet que estão sujeitos às ações dos órgãos públicos são: "fornecedores de acesso, conteúdos e centro de dados da internet e serviços de nome de domínio; provedores de serviços de informações da Internet; prestadores de serviços públicos de internet; e prestadores de serviços de internet em geral" (MINSTRY OF PUBLIC SECURITY, 2018, p. 2, tradução nossa)[55].

Ou seja, praticamente todos os serviços relacionados à internet no país ficam expostos aos órgãos públicos, sendo definido que os conteúdos informacionais armazenados e compartilhados que o órgão competente considera suspeitos podem ser examinados. A convocação da supervisão ocorre quando há a prerrogativa de manter a segurança das redes de informação ou em momentos de importantes tarefas nacionais de defesa e segurança cibernética (MINISTRY OF PUBLIC SECURITY, 2018). As agências estatais também possuem obrigações legais na execução de sua função, como prezar pela privacidade de determinadas informações e dados e não os comercializar, mantendo a confidencialidade requisitada, bem como não abusar de seu poder. Fica previsto também, multas e punições para aqueles que desrespeitarem as cláusulas estabelecidas e não colaborarem com as inspeções remotas feitas.

Além disso, há o documento denominado de "Medidas de Gerenciamento de Segurança de Dados"[56] (2019), que apresenta artigos que definem como a coleta e o gerenciamento de dados devem ser feitos pelos operadores de redes de informação na China. Em especial as obrigações e responsabilidades que devem ter em relação aos dados e informações pessoais, seguindo condutas de respeito às éticas sociais chinesas. É determinado, por exemplo, como os operadores de rede e pessoas encarregadas pela segurança dos dados devem conduzir e organizar os planos de proteção de dados, a avaliação de riscos da segurança das informações, como reportar aos departamentos governamentais superiores as medidas de proteção e segurança cibernética feitas, entre outros (NATIONAL INTERNET INFORMATION OFFICE, 2019).

---

[54] Texto original: **公安机关互**联网安全监督检查规定.

[55] Texto original: **提供互**联网接入、互联网数据中心、内容分发、域名服务的；提供互联网信息服务的; 提供公共上网服务的; 提供其他互联网服务的。

[56] Texto original: **数据安全管理**办法.

Por fim, o mais recente documento estratégico voltado para a defesa nacional outorgado pela China é o "Defesa Nacional da China na Nova Era"[57] (2019). Nele, o governo analisa que o poder estratégico dos países está ficando cada vez mais balanceado no contexto internacional. É argumentado que há uma intensificação pela competição militar com o desenvolvimento de novos tipos de forças de combate e um maior engajamento de grandes potências em inovação tecnológica e institucional, na busca por uma superioridade militar absoluta.

> A competição militar internacional está passando por mudanças históricas. Novas e elevadas tecnologias militares baseadas em TI estão se desenvolvendo rapidamente. Existe uma tendência predominante de desenvolver armas e equipamentos de precisão, inteligência, furtivos ou não tripulados de longo alcance (STATE COUNCIL INFORMATION OFFICE, 2019, p. 6, tradução nossa)[58].

Com isso, para proteger os interesses e objetivos chineses para a nova era, a estratégia de defesa nacional se apoia no domínio cibernético, tanto para proteger a nação de ameaças externas e diminuir as vulnerabilidades dos sistemas e redes de informação que afetam a segurança nacional, quanto para atingir a completa modernização do setor militar até o ano de 2035 (STATE COUNCIL INFORMATION OFFICE, 2019). O ciberespaço, a ciberdefesa e a cibersegurança, portanto, são vistas como um desafio global. O documento reitera, em concordância com os demais documentos, a ideia de que é necessária a construção de melhores capacidades cibernéticas, consistentes com o status internacional da China de potência cibernética, de modo a reforçar a defesa das fronteiras nacionais do ciberespaço, detectar e conter intrusos nas redes e sistemas, de modo a salvaguardar a segurança das informações, mantendo a soberania cibernética e a estabilidade social da nação.

3.3 Israel

O governo israelense iniciou a regulamentação e a determinação da sua estratégia nacional cibernética mais tarde que EUA e China, apenas no ano de 2011 a primeira resolução sobre o assunto foi formulada. Identificada como "Resolução 3611"[59] (2011), ela conceitua os principais termos cibernéticos na visão de Israel, servindo como uma espécie de introdução ao tema para o país. Nela, o ciberespaço, por exemplo, é definido como um ambiente composto por aspectos físicos e não físicos, formado por fatores como sistemas de computadores, redes

---

[57] Texto original: China's National Defense in the New Era

[58] Texto original: International military competition is undergoing historic changes. New and high-tech military techonologies based on IT are developing rapidly. There is a prevailing trend to develop long-range precision, intellingent, stealthy or unmanned weaponry and equipment

[59] Texto original: 3611 של הממשלה מיום.

de comunicação, softwares, conteúdos transmitidos por computadores, informações computadorizadas e o tráfego e controle de dados e usuários (PRIME MINISTER'S OFFICE, 2011). Nesse sentido, a cibersegurança seria as políticas, mecanismos, ferramentas e medidas formuladas e tomadas para proteger o ciberespaço e habilitar o seu uso (PRIME MINISTER'S OFFICE, 2011).

A resolução inaugura as diretrizes que o Estado de Israel decidiu tomar para que a segurança dos seus sistemas e redes de informação fossem asseguradas, primando pela proteção das infraestruturas essenciais para a existência de uma vida normal no país, pela máxima prevenção de ataques cibernéticos e almejando a promoção do status de Israel como um centro de desenvolvimento tecnológico, principalmente por meio da colaboração entre Estado, setor privado e a academia (PRIME MINISTER'S OFFICE, 2011).

O documento é introdutório, servindo como uma apresentação das intenções do governo para a implementação de uma segurança cibernética eficaz no país, sem especificar de que forma isso irá ocorrer. É também responsável pelo estabelecimento de departamentos governamentais, como o *Israel National Cyber Bureau* (INCB), especializado no setor cibernético, determinando suas funções e competências perante o poder público, tais como a recomendação de políticas nacionais, aconselhamento ao primeiro ministro, fomento ao desenvolvimento de capacidades cibernéticas, entre outros (PRIME MINISTER'S OFFICE, 2011).

Fica elucidado também a necessidade de aprimorar soluções de defesa local, adaptar a organização estrutural do país e desenvolver tecnologias que contribuam para a segurança cibernética, encorajando as indústrias nacionais. O objetivo maior esclarecido na Resolução 3611 (2011) é o de construir meios para o uso inteligente do ciberespaço, por meio de programas, ações coordenadas, colaborações, que permitam uma abordagem eficaz contra incidentes e emergências cibernéticas que podem acontecer em Israel. Ou seja, construir um Estado que esteja preparado para conduzir ações nacionais e internacionais capazes de lidar com imprevistos, ataques e ameaças no ciberespaço.

No ano de 2015, o governo de Israel promulgou a "Resolução 2443"[60] (2015), destinada à população e aos setores econômicos e de mercado do país, para se adaptarem aos princípios das políticas nacionais em segurança cibernética formuladas pelo INCB. Possuindo um caráter de reforço às regulamentações na área cibernética iniciadas em 2011, o intuito dessa resolução é regularizar serviços e produtos, incluindo profissionais e o comércio de segurança

---

[60] Texto original: Resolution No. 2443.

cibernética no país (THE GOVERNMENT SECRETARY, 2015a). Foi responsável também pela fundação do *National Cyber Security Authority* (NCSA) como o departamento governamental responsável por coordenar os regulamentos e colocar os planos de ação em prática (THE GOVERNMENT SECRETARY, 2015a). A criação do NCSA propiciou a fundação, pelo governo, do *Israeli National Cyber Directorate*, convergindo o INCB e o NCSA sob sua tutela e a uma mesma coordenação nacional.

O Estado de Israel se mostra preocupado com a regularização de um mercado cibernético emergente de serviços e produtos. Por isso, a missão determinada pela Resolução 2443 (2015) é guiar e instruir as agências e escritórios governamentais em aspectos como o gerenciamento de riscos, mapeamento de objetos vulneráveis, elaboração de um plano de segurança cibernética e a alocação de recursos para implementá-lo (THE GOVERNMENT SECRETARY, 2015a). Para isso é expressado a importância da formulação de políticas, métodos de trabalho e preparação para lidar com acidentes cibernéticos, no intuito de tornar o país apto para recuperação e reabilitação em casos de incidentes.

As atividades cibernéticas no país são compreendidas na resolução como importantes fatores para o avanço econômico e social da nação, devendo ser realizadas de maneira formal, contribuindo para elevar o nível de capacitação contra ameaças cibernéticas, seguindo uma lógica semelhante aos discursos adotados pelos EUA e também pela China. Também são estipulados na Resolução 2443 (2015) os recursos humanos e orçamentários destinados aos programas de regulamentação das atividades de segurança cibernética e aos escritórios e departamentos estatais competentes.

Ainda no ano de 2015, o governo de Israel outorgou a “Resolução 2444”[61] (2015), visando a promoção da preparação nacional para a proteção cibernética, que estabeleceu as funções reservadas para o *Cyber Emergency Response Team* (CERT) de Israel e orquestrou as estruturas de autoridade e responsabilidades dos departamentos estatais ligados à defesa cibernética nacional. A NCSA ficou encarregada de operar a CERT, que passou a ser o principal centro de assistência para civis na área cibernética de Israel, sendo incumbido de lidar com incidentes cibernéticos, promovendo atividades de coordenação entre indústrias e o governo israelense, trabalhando com a prevenção contra acidentes cibernéticos, compartilhamento de informações relevantes, entre outros (THE GOVERNMENT SECRETARY, 2015b).

Além dessas resoluções, o poder público de Israel estabeleceu a sua estratégia nacional para o ciberespaço em dois principais documento oficiais, a “Estratégia Nacional de Segurança

---

[61] Texto original: Resolution No. 2444.

Cibernética de Israel em Resumo"[62] (2017) e a "Estratégia Oficial das Forças de Defesa de Israel"[63] (2016), este publicado no ano de 2015 e traduzido pela *Havard Kennedy School* em 2016. Assim como os outros dois países anteriormente analisados, Israel reconhece que a doutrina formulada se baseia no entendimento de que o mundo mudou e as ameaças que as nações enfrentam não são mais apenas as ameaças convencionais. A estratégia consiste em construir e manter o ciberespaço seguro em consonância com os interesses nacionais do país, com o objetivo maior de assegurar o papel do Estado de Israel como um líder internacional em inovação tecnológica, sendo um parceiro global ativo no processo de moldar o ciberespaço (PRIME MINISTER'S OFFICE, 2017).

Ambos os documentos expressam a concepção de Israel sobre segurança nacional, fortemente influenciada pela realidade regional no qual o país está inserido. Essa concepção é baseada em alguns pontos principais, como a dissuasão, a advertência ou aviso prévio e a vitória operacional decisiva (BARAM, 2017). Os desafios que o desenvolvimento tecnológico vem trazendo nos últimos anos para o conceito tradicional de segurança fizeram com que as Forças de Defesa de Israel (IDF) se adaptassem e desenvolvessem novos equipamentos e armas, fazendo do IDF o mais avançado exército do Oriente Médio (BARAM, 2017).

A Estratégia Oficial das Forças de Defesa de Israel (2016) é descrita como a fundamentação conceitual e prática para todos os documentos militares bases do país, sustentado pelos princípios da doutrina da segurança nacional, que são: a confiança na estratégia de defesa e segurança; ter uma concepção ofensiva dos assuntos militares; buscar uma cooperação estratégica; fortalecer o status regional de Israel e manter o relativo avanço da nação (ISRAEL DEFENSE FORCES, 2016). Esses princípios servem para a proteção do Estado de Israel contra seus inimigos estatais e não estatais declarados no documento, sendo eles: Irã, Líbano, Síria, Hezbollah, Hamas, ISIS e o Movimento da Jihad Islâmica na Palestina.

No que tange as áreas de um conflito, o documento expressa a firme posição do país em manter a continuidade dos esforços econômicos e de guerra por todas as dimensões eficazes de defesa nacional, incluindo o ciberespaço, como forma de garantir a superioridade militar israelense para atingir os seus objetivos e garantir seus interesses (ISRAEL DEFENSE FORCES, 2016). Profere-se que esforços ofensivos no setor cibernético serão utilizados para situações de emergência e de guerra, ressaltando-os como um importante meio para todos os níveis de um combate – estratégico, operacional e tático – pois, a missão maior do IDF é

---

[62] Texto original: Israel National Cyber Security Strategy in Brief
[63] Texto original: Official Strategy of the Israel Defense Forces

defender o território e a soberania de Israel, sendo o ciberespaço reconhecido como um domínio capaz de assegurar essa finalidade (ISRAEL DEFENSE FORCES, 2016).

A segurança cibernética do país prima por defender organizações, o governo, as infraestruturas críticas, o setor privado e os cidadãos israelenses. O IDF reconhece que praticamente todas as armas militares hoje em dia, incluindo submarinos e mísseis, possuem componentes eletrônicos que podem ser vulneráveis à ataques através do ciberespaço e, consequentemente, preza por desenvolver capacidades suficientes para defender as redes de comunicação e os sistemas militares e governamentais, sempre considerados alvos em potencial (COHEN et al., 2016). Assume-se, portanto, que Israel considera a proteção mais importante do que lidar com o perpetrador da agressão, concentrando seu foco no preparo das capacidades para enfrentar todas as possibilidades de ataques em qualquer setor (ADAMSKY, 2017).

Com essa conduta, o governo israelense projeta, na Estratégia Nacional de Segurança Cibernética de Israel em Resumo (2017), estruturar com eficiência empenhos que garantam uma solução estável para os perigos e riscos que o mal uso do ciberespaço pode acarretar para a segurança nacional. A operacionalização estratégica do desenvolvimento cibernético é definida no documento em três camadas hierárquicas: (i) Agregar Robustez Cibernética, (ii) Resiliência Cibernética Sistêmica e (iii) Defesa Cibernética Nacional (PRIME MINISTER'S OFFICE, 2017). A premissa consiste em unir as naturezas e características do ciberespaço, abrangendo suas ameaças e riscos, com os papéis que o setor público e o setor privado devem desempenhar para alcançar a segurança cibernética nacional. As camadas divergem uma das outras no que concerne aos seus objetivos específicos, mas as suas ações e medidas possuem a mesma meta final: a defesa e a segurança nacional.

A primeira camada, denominada de Agregar Robustez Cibernética, se caracteriza por ser a habilidade das organizações e processos de continuar operando apesar de uma rotina de ameaças, repelindo e prevenindo a maioria dos ataques (PRIME MINISTER'S OFFICE, 2017). Essa robustez é alcançada, segundo o documento, por meio de melhores práticas, orientações, regulamentações, incentivos das organizações responsáveis e pela regulação do mercado de segurança cibernética. Na questão de regulação de um mercado comercial para a segurança cibernética, são elencados pontos considerados cruciais para a sua ocorrência e formalização, como profissionais cibernéticos, produtos e serviços securitários, serviços tecnológicos, orientações específicas para as infraestruturas críticas, normas obrigatórias em setores essenciais e a promoção de conhecimento e conscientização por meio do setor privado (PRIME MINISTER'S OFFICE, 2017).

Setor este constituído de aproximadamente 360 empresas no ramo da segurança cibernética em Israel e que representou uma estimativa de US$ 6 bilhões em exportações de produtos cibernéticos no ano de 2016 (COURIEL, 2017). A relação público-privado em Israel é muito forte e faz com que na área tecnológica o país seja um polo mundial. Mais de 30 multinacionais identificaram o país como o melhor local para desenvolvimento de capacidade e conhecimento na área de segurança cibernética, atraindo um investimento global privado de aproximadamente meio bilhão de dólares por ano, fazendo com que o país fique apenas atrás dos Estados Unidos nesse quesito (ADAMSKY, 2017). Para a construção de capacidades cibernéticas de alto nível, os esforços do Estado de Israel são direcionados para a área de Pesquisa e Desenvolvimento (P&D), cultivando o capital científico-tecnológico do país (ADAMSKY, 2017).

O segundo nível relatado na estratégia nacional, a Resiliência Cibernética Sistêmica, é descrita como a capacidade de confrontar ataques cibernéticos antes, durante e depois de acontecerem, de maneira a prevenir que suas consequências se alastrem, com o objetivo claro de reduzir ao máximo os custos e os danos desses ataques e incidentes à nação (PRIME MINISTER’S OFFICE, 2017). Essa camada estratégica é diretamente voltada para a ocorrência de eventos. Presume-se que a resiliência pode ser alcançada por meio da geração e compartilhamento de informações valiosas em conjunto com a assistência às organizações durante um incidente cibernético, realizando essas operações de maneira coordenada, como engrenagens de um mesmo sistema (PRIME MINISTER’S OFFICE, 2017).

Na terceira e última camada, o considerado topo da pirâmide, está a Defesa Nacional Cibernética, sendo configurada como uma convergência nacional contra ameaças cibernéticas que coloquem o Estado de Israel em perigo. É baseada na promoção de uma campanha de defesa nacional que deve ser feita pelo Estado, em um esforço ativo para confrontar a fonte das ameaças e a suas ramificações (PRIME MINISTER’S OFFICE, 2017). O documento divide essa estratégia em duas áreas que se intersectam. Uma área representa as campanhas contra agressores, composta por inteligência, prevenção, execução e dissuasão; a outra são as campanhas de defesa nacional, composta por operações defensivas, respostas nacionais à incidentes e a avaliação da situação. A intersecção das áreas das campanhas é definida como as investigações conjuntas que devem ser feitas (PRIME MINISTER’S OFFICE, 2017).

A agência estatal que chefia as operações estratégicas das três camadas é o NCSA, servindo como um eixo do conhecimento nacional em segurança cibernética e um centro de gerenciamento para os incidentes cibernéticos no país, sempre cooperando de maneira aberta com o setor privado. O empenho está centrado na finalidade de manter Israel na vanguarda

global da produção de conhecimento científico-tecnológico na área de segurança e defesa cibernética. Dessa forma, como aspecto da estratégia nacional, a cultura da inovação é fomentada, criando um ambiente cibernético que atenda às necessidades locais e globais do país. Essa prioridade de reforçar as capacidades cibernéticas israelenses, já estabelecida desde a Resolução 3611 (2011), ganha dois elementos imprescindíveis na Estratégia Nacional de Segurança Cibernética de Israel em Resumo (2017).

O primeiro é a pesquisa, desenvolvimento e implantação de capacidades e tecnologias de segurança cibernética à nível nacional, incluindo plataformas de compartilhamento de informações, serviços de segurança centralizados e soluções que apoiem os esforços do Estado em investigar e conter ataques cibernéticos (PRIME MINISTER’S OFFICE, 2017). O segundo concerne no fortalecimento da área de ciência e tecnologia no país, baseado na fomentação de inovações industriais, no suporte à pesquisa acadêmica, no aprimoramento do capital humano no setor cibernético e viabilização de um ecossistema de benefícios mútuos (PRIME MINISTER’S OFFICE, 2017). O documento ainda destaca o projeto *CyberSpark*, que consiste justamente na colaboração coordenada entre o Estado, a academia, a indústria, principalmente as *startups* israelenses, e o setor militar na formulação saudável de um espaço cibernético seguro e confiável.

O capital humano, elucidado como um dos fatores para o aperfeiçoamento das capacidades cibernéticas do Estado de Israel, é enfatizado também em um documento oficial específico, intitulado de “Políticas de Regulamento de Profissões de Segurança Cibernética no Estado de Israel”[64] (2015). O documento regula, de maneira formal, algumas profissões relacionadas à cibersegurança. O propósito exposto pelo governo é o de apresentar as áreas e disciplinas a serem reguladas, o conhecimento requisitado para os profissionais e os mecanismos da regulamentação. Todo o processo de aprendizado e qualificação da profissão é esclarecido. O documento traz as validações das áreas, a preparação para os testes de conhecimento, define condições e processos para receber e renovar os certificados e também as competências necessárias para os testes (PRIME MINISTER’S OFFICE, 2015).

A importância do capital humano no país pode ser notada quantitativamente. “Israel é o país com maior concentração de engenheiros no mundo em sua população, cerca de 135 para cada 10,000 pessoas, comparado com 85 para cada 10,000 pessoas nos Estados Unidos, que figura na segunda colocação” (TABANSKY; BEN-ISRAEL, 2015, p. 19, tradução nossa)[65].

---

[64] Texto original: מדיניות אדסרת מקצועות הגנת הסייבר במדינת ישראל.

[65] Texto original: Israel has the highest concentration of engineers in the world – 135 per 10,000 people, compared to 85 per 10,000 people in the United States which stands in the second place.

Além disso, as universidades do país estão entre as 50 melhores instituições acadêmicas do mundo nas áreas de química, matemática, ciências naturais e engenharia, sendo que todas possuem companhias de transferência tecnológica, que provê a estrutura legal e a proteção, por meio de patentes, da comercialização de produtos, equipamentos e invenções feitas pelos estudantes e pesquisadores (TABANSKY; BEN-ISRAEL, 2015).

As características da área de segurança cibernética requerem conhecimentos, segundo o documento de 2015, em uma grande variedade de assuntos: como administração, ciência da computação, sistemas da informação, engenharia da computação, matemática, saber lidar com hardware, software, comunicação, banco de dados, operar sistemas, entre outros (PRIME MINISTER’S OFFICE, 2015). O documento também destaca que muitos países no mundo já estão aperfeiçoando a sua mão de obra para o setor cibernético, como os EUA, Singapura, Reino Unido e Austrália. Dessa forma, o governo israelense analisa que precisa acelerar o desenvolvimento das habilidades da sua sociedade para conseguir competir economicamente em nível global (PRIME MINISTER’S OFFICE, 2015). São cinco profissões regulamentadas no documento: Praticante de Segurança Cibernética, Especialista em testes de penetração Cibernética, Especialista Forense Cibernético, Especialista em Metodologia de Segurança e Especialista em Tecnologia de Segurança Cibernética (PRIME MINISTER’S OFFICE, 2015, n.p, tradução nossa)[66].

Fica declarado também as características de cada profissão, assim como os conhecimentos teóricos e práticos necessários, os principais princípios que devem ser seguidos e os exames que devem realizar para obter o certificado oficial válido por três anos. O objetivo do governo de Israel é implementar a regularização dessas profissões até 2021, estando prontas para atuar no mercado de trabalho nacional (PRIME MINISTER’S OFFICE, 2015). A conscientização da sociedade civil para a segurança cibernética, portanto, é colocada em prática pelo Estado através da normatização de atividades que envolvam o ciberespaço. Tudo isso com a meta central de desenvolver as TICs nacionais, aumentando a capacidade de proteção do espaço virtual e das infraestruturas críticas do país.

Por fim, no âmbito internacional, o Estado de Israel, em consonância com EUA e China, também preza pela cooperação multilateral na esfera do ciberespaço como forma de estabelecer um ambiente cibernético seguro mundialmente. Contudo, se aproxima da posição estadunidense em priorizar esforços e trabalhos conjuntos com os seus parceiros estratégicos,

[66] Texto original: Cyber Security Practitioner, Cyber Penetration Testing Specialist, Cyber Forensic Specialist, Cyber Security Methodology Specialist e Cyber Security Technology Specialist.

para fortalecer as suas capacidades cibernéticas nacionais, bem como a dos seus aliados. "Israel convida parceiros ao redor do mundo para trabalharem juntos, para compartilhar conhecimento para o desenvolvimento de novas soluções à nível global e para preencher nossa compartilhada visão de um ciberespaço seguro e próspero" (PRIME MINISTER'S OFFICE, 2017, p. 18, tradução nossa).[67]

3.4 Considerações sobre as estratégias de EUA, China e Israel

A partir da análise descritiva dos documentos oficiais citados, pode-se inferir que o ciberespaço, a defesa e a segurança cibernética foram ganhando relevância para os três países com o passar dos anos. Todos justificam as suas políticas e estratégias cibernéticas adotadas em vista das grandes ingerências das tecnologias da informação e comunicação na vida dos seus cidadãos, na realização de suas atividades básicas, e, consequentemente na necessidade do Estado em atuar para garantir um ambiente de fluxos de informações seguro e confiável.

Estados Unidos, China e Israel reconhecem essa necessidade de atuação em vista da emergência das ameaças que o espaço cibernético propiciou, podendo afetar diretamente a defesa e a segurança nacional. Destaca-se, nesse sentido, que há muitas semelhanças entre os elementos que são considerados essenciais pelos três países para se atingir uma defesa e segurança cibernética consideradas ideais. Entre os elementos, destacam-se o foco na proteção das infraestruturas críticas, o apoio estratégico na aproximação entre o setor público e o setor privado, o fomento no desenvolvimento e inovação de tecnologias, especialmente as TICs, a cooperação internacional e o reconhecimento do capital humano como indispensável para que os objetivos traçados sejam alcançados.

Esses fatores chaves foram encontrados nas estratégias cibernéticas dos três países analisados, podendo indicar um possível padrão de identificação dos principais pontos vistos como estratégicos para o aperfeiçoamento da defesa e da segurança cibernética. Dessa forma, o que diferencia cada país é a forma abordada sobre como lidar com esses fatores chaves. A China, pela característica mais centralizadora na forma de governar, possui uma abordagem que concentra os esforços do país a partir do monitoramento, suporte e supervisão dos departamentos estatais. O poder do Estado chinês na implementação das ações e medidas no país são realçados nos documentos, ficando a cargo dos proprietários das infraestruturas críticas

[67] Texto original: Israel invites partners around the world to work together to share knowledge, to develop new solutions on the global level and to fulfill our shared vision of a secure and prosperous cyberspace.

e das redes de comunicação, por exemplo, se submeterem às determinações e a supervisão do governo.

Já no caso dos Estados Unidos e Israel, há certa semelhança entre eles também nas suas abordagens em relação aos esforços e implementação de medidas perante os elementos chaves comentadas. Nota-se uma aproximação na forma como o governo estadunidense e o governo israelense enxergam como as ações devem ser tomadas no âmbito cibernético, prezando pela boa relação entre as instituições públicas e privadas na busca pelo aprimoramento de suas capacidades cibernéticas.

Será dado um maior destaque e aprofundamento sobre as diferenças e aproximações entre os três países no próximo capítulo, de modo a realçar as suas ações estratégicas práticas. Por enquanto, de maneira geral, pode-se considerar que a principal divergência encontrada entre Estados Unidos, China e Israel está na forma como lidam com os aspectos que consideram vitais para estabelecer a segurança cibernética em seus países e não nos aspectos em si, evidenciando uma divergência na visão política que possuem sobre o ciberespaço, que termina por guiar as ações a serem implementadas por cada um.

Tabela 1 - Documentos estratégicos analisados

País	Documento	Data	Órgão responsável
Estados Unidos	Estratégia Nacional para Proteger o Ciberespaço	2003	White House
	Revisão da Política para o Ciberespaço	2009	White House
	Estratégia Militar Nacional dos Estados Unidos da América	2011	Joint Chiefs of Staff
	Plano Nacional de Proteção a Infraestrutura (NIPP)	2013	Department of Homeland Security
	Estratégia de Segurança Nacional dos Estados Unidos da América	2017	White House
	Estratégia Cibernética Nacional dos Estados Unidos da América	2018	White House
	Resumo da Estratégia Cibernética	2018	Department of Defense

	Estratégia de Segurança Cibernética do Departamento de Segurança Interna dos Estados Unidos	2018	Department of Homeland Security
	Resumo da Estratégia de Defesa Nacional dos Estados Unidos da América	2018	Department of Defense
	Estratégia Nacional de Inteligência dos Estados Unidos da América	2019	Intelligence Community
	Dicionário do Departamento de Defesa sobre Termos Militares e Associativos	2020	Department of Defense
República Popular da China	Pareceres do Grupo de Liderança Nacional em Informatização sobre Fortalecimento da Segurança da Informação	2003	Government of the Popular Republic of China
	Pareceres da Comissão Militar Central solicitando maior fortalecimento da segurança militar da informação	2014	Cyberspace Administration of China
	Estratégia Nacional para a Segurança no Ciberespaço	2016	Cyberspace Administration of China
	Lei de Segurança Cibernética da República Popular da China	2016	Office of the Central Cyberspace Affairs Commission
	Estratégia Internacional de Cooperação no Ciberespaço	2017	Ministry of Foreign Affairs
	Regulamentos sobre a Proteção do Direito de Comunicação na Rede de Informações	2017	Ministry of Industry and Information Technology
	Regulamentos sobre o Gerenciamento de Serviços Comerciais de acesso à Internet	2017	Ministry of Industry and Information Technology
	Disposições sobre Supervisão e Inspeção de Segurança na Internet por Órgãos de Segurança Pública	2018	Ministry of Public Security
	Medidas de Gerenciamento de Segurança de Dados	2019	National Internet Information Office

	Defesa Nacional da China na Nova Era	2019	State Council Information Office
Israel	Resolução 3611	2011	Prime Minister's Office
	Resolução 2443	2015	The Government Secretary
	Resolução 2444	2015	The Government Secretary
	Políticas de Regulamento de Profissões de Segurança Cibernética no Estado de Israel	2015	Prime Minister's Office
	Estratégia Oficial das Forças de Defesa de Israel (IDF)	2016	Israel Defense Forces (IDF)
	Estratégia Nacional de Segurança Cibernética de Israel em Resumo	2017	Prime Minister's Office

Fonte: Elaborado pelo autor

4 A PERSPECTIVA CIBERNÉTICA BRASILEIRA E AS SUAS DIVERGÊNCIAS E APROXIMAÇÕES COM AS ESTRATÉGIAS DE EUA, CHINA E ISRAEL

Após a análise dos documentos oficiais dos respectivos países, nesta seção será observado as propostas estratégicas do Brasil em relação à defesa e segurança cibernética, por meio dos documentos oficiais publicados até então. O país sul americano é a maior economia de sua região, possuindo características continentais em relação ao seu território, população e recursos. Entretanto, segundo o *Global CyberSecurity Index* (2018), o Brasil configura a 70ª posição global em segurança cibernética e se localiza na 4ª posição no rank regional quando comparado aos demais países latino americanos, ficando atrás de Uruguai, México e Paraguai, respectivamente. A dificuldade de estabelecer uma plena segurança cibernética pode se encontrar justamente na grande extensão e diversidade que o país possui, mas também pode estar na ausência de uma articulação nacional para determinar diretrizes e estratégias cibernéticas nacionais no país.

Conforme comentado anteriormente, a falta de normas internacionais específicas para o ciberespaço permite que os Estados adotem políticas e medidas próprias para proteger esse espaço. E a adoção de políticas e estratégias cibernéticas tiveram o seu início em países mais desenvolvidos tecnologicamente, nos quais suas sociedades já estavam mais conectadas e dependentes aos meios digitais. A urgência do tema em nações com essas características é maior e, consequentemente, ações e regulamentos legais emergem na tentativa de tornar essa nova realidade segura e benéfica para o país, gerando uma certa divisão digital entre os países desenvolvidos e não desenvolvidos. Segundo a OCDE, a divisão digital:

> [...] refere-se à lacuna entre indivíduos, famílias, negócios e áreas geográficas em diferentes níveis socioeconômicos no que diz respeito às suas oportunidades de acesso a tecnologias de informação e comunicação e ao uso que fazem da internet para uma ampla variedade de atividades (OCDE, 2001, p. 5, tradução nossa)[68].

Nesse contexto global de desigualdades tecnológicas, muitos pesquisadores têm destacado a complexidade e a multidimensionalidade das variáveis da divisão digital, como diferenças educacionais, culturais, institucionais, sociodemográficas e políticas (BILLON et al. 2010). Dessa forma, além da análise dos documentos brasileiros oficiais, nesta seção também consta uma breve discussão crítica sobre os quatro países abordados neste trabalho, buscando não só comparar as iniciativas e medidas tomadas por cada um, mas também tentando avaliar

---

[68] Texto original: [...] refers to the gap between individuals, households, business and geographic areas at different socio-economic levels with regard both to their opportunities to access information and communication Technologies (ICTs) and to their use of the Internet for a wide variety of activities.

se há uma certa influência das estratégias cibernéticas das potências estrangeiras nas concepções sobre ciberespaço, defesa e segurança cibernética de um país mais periférico no sistema internacional, como o Brasil, que começou a se digitalizar mais tarde e possui um gap tecnológico em relação aos Estados Unidos, China e Israel.

4.1 Brasil

A percepção do setor cibernético como um elemento chave para a defesa e a segurança nacional do Brasil se materializou em 2008 com a elaboração da Estratégia Nacional de Defesa (END), que no ano de 2012 foi revisada, atualizada e publicada conjuntamente com a Política Nacional de Defesa (PND). O documento eleva o setor cibernético como um dos três setores estratégicos para a defesa do país, junto com o setor nuclear e espacial, com base na concepção de que a segurança é a condição em que o Estado, sociedade ou indivíduos se sentem livres de riscos e que a defesa é a ação para se obter o grau de segurança desejado (MINISTÉRIO DA DEFESA, 2012a).

Importante destacar que a Política Nacional de Defesa e a Estratégia Nacional de Defesa sofreram dois processos de atualização desde 2012. A primeira ocorreu em 2016 e a segunda em 2020. Contudo, apesar de elaboradas e apresentadas, ambas as atualizações não foram homologadas. Dessa forma, a versão de 2012 está em vigor até os dias de hoje e, por isso, foi a única edição utilizada neste trabalho.

A PND/END (2012) esclarece que o desenvolvimento e a capacitação tecnológica, juntamente com o domínio de tecnologias sensíveis, são indispensáveis para a independência nacional nos setores estratégicos citados (MINISTÉRIO DA DEFESA, 2012a). O fortalecimento do setor cibernético por meio do aperfeiçoamento de tecnologias, principalmente de informação e comunicação, é exposto como uma ação necessária para que o Brasil não dependa de capacidades estrangeiras e possa garantir a sua soberania. Além disso, os instrumentos cibernéticos são tidos como especiais, por serem necessários para assegurar comunicações entre os equipamentos dos setores aéreo, espaciais e terrestre (MINISTÉRIO DA DEFESA, 2012a).

Em busca da estabilidade e do desenvolvimento, o documento instiga o fortalecimento do Centro de Defesa Cibernética (CDCiber) e o aprimoramento da segurança da informação e comunicação (SIC), especialmente no que tange as infraestruturas críticas do país. Assim, o desenvolvimento tecnológico é elencado como uma prioridade estratégica pela PND/END (2012), devendo ser fomentado por meio da pesquisa científica voltada para o setor cibernético,

no intuito de incrementar os sistemas baseados em computação e aprimorar a capacidade cibernética operacional e estratégica do país dentro do ciberespaço.

No ano de 2010, dois anos após a primeira edição da END, o governo federal brasileiro, por meio do Gabinete de Segurança Institucional (GSI), elaborou o Livro Verde sobre segurança cibernética no Brasil. O objetivo da obra era estabelecer uma política nacional de segurança cibernética com visões de curto, médio e longo prazo. Com uma justificativa semelhante ao dos países analisados no segundo capítulo, é expressado que devido a grande velocidade com que os avanços tecnológicos vêm afetando a sociedade como um todo, é preciso que haja um rearranjo nas ideias das nações em termos de segurança e defesa (GABINETE DE SEGURANÇA INSTITUCIONAL, 2010).

O livro dedica uma boa parte dos seus capítulos iniciais para enfatizar as iniciativas que o Brasil tomou em organismos internacionais, assim como propostas na qual foi signatário. De forma a demonstrar o interesse e a importância que o governo brasileiro estava dando para o assunto cibernético, traz-se exemplos em que o país teve participações ativas na construção de bases multilaterais para o entendimento sobre segurança cibernética. Entre os casos citados, destaca-se a proposta feita em 2010 por uma nova convenção de caráter global sobre crime cibernético, elaborada pelos países do BRICS (Brasil, Rússia, Índia, China e África do Sul), com a intenção de expandir e aprimorar a Convenção de Budapeste, a única convenção internacional que trata sobre o tema (GABINETE DE SEGURANÇA INSTITUCIONAL, 2010)

É exposto preocupação com o ambiente internacional em relação ao setor cibernético e comenta-se que muitas economias desenvolvidas já estavam revisando e avançando as suas estratégias nacionais de defesa e segurança cibernética, como os Estados Unidos e o Reino Unidos (GABINETE DE SEGURANÇA INSTITUCIONAL, 2010). Dessa forma, o governo brasileiro vê essa tendência como a sinalização de que muito esforço e trabalho devem ser dispendidos nessa área, principalmente em termos de cooperação internacional, legislação nacional e internacional, normatização e capacitação de recursos humanos (GABINETE DE SEGURANÇA INSTITUCIONAL, 2010).

De modo geral, o livro institui a visão do Brasil sobre os pontos político-estratégico que considera mais importantes em relação à segurança cibernética. São considerados como mais importantes os setores no qual a questão cibernética afeta de maneira direta ou indireta, como o setor econômico, socioambiental, educacional, legal, ciência, tecnologia e inovação (CT&I) e a segurança das infraestruturas críticas. No âmbito econômico, evidencia-se a ascensão do comércio digital, representando uma proporção cada vez maior nos totais das vendas

transacionadas no país, bem como o potencial aumento na criação de empregos formais dentro do setor cibernético (GABINETE DE SEGURANÇA INSTITUCIONAL, 2010). Alguns desafios nos setores citados também são listados pelo governo, como por exemplo, o insuficiente monitoramento e proteção dos recursos naturais do país na questão ambiental; a carência de programas que promovam o desenvolvimento tecnológico no âmbito da CT&I; a incipiente formação de técnicos e especialistas em cibernética no âmbito educacional; entre outros (GABINETE DE SEGURANÇA INSTITUCIONAL, 2010).

À vista disso, o Livro Verde traz diretrizes para serem implementadas em cada um dos setores destacados como parte da construção de política nacional de segurança cibernética. Dentre elas, destaca-se: categorizar a segurança cibernética como alta prioridade e urgência para o país; incrementar a capacidade dissuasória de defesa; promover a regulação do mercado digital; estreitar parcerias entre o setor público e privado; desenvolver programas de inclusão digital; incluir temas que envolvam o ciberespaço nos currículos de ensino fundamental e médio do país; articular o fortalecimento da ciência e pesquisa no âmbito cibernético; promover a cooperação bilateral e multilateral em segurança cibernética; mapear o grau de vulnerabilidades das infraestruturas críticas, entre outras. (GABINETE DE SEGURANÇA INSTITUCIONAL, 2010).

Além disso, o Livro Branco de Defesa Nacional publicado em 2012 também configura o setor cibernético como um setor estratégico para a defesa do país. Apesar de não abordar de maneira extensa sobre a questão cibernética, o documento expressa a preocupação que as ameaças cibernéticas trouxeram para integridade das infraestruturas críticas e essenciais para a operação e controle dos sistemas e órgãos voltados para a segurança nacional (BRASIL, 2012). Assim, o livro determina alguns objetivos e ações de curto prazo para o projeto de defesa cibernética e do fortalecimento do CDCiber. Como fomentar a base industrial de defesa, induzir a inovação tecnológica, adquirir soluções de software e hardware de defesa cibernética, melhorar a capacitação dos recursos humanos, fortalecer a segurança e a proteção contra ataques cibernéticos e construir a sede definitiva do CDCiber (BRASIL, 2012). O período previsto para a conclusão total do projeto é em 2035 e o valor estimado é de R$ 839, 90 milhões.

Dessa forma, a compreensão estratégica assumida pelo governo brasileiro agilizou algumas medidas governamentais, especialmente voltadas para o setor militar na proteção do ciberespaço. No mesmo ano de 2012, foi publicada a Política Cibernética de Defesa e, em 2014, a Doutrina Militar de Defesa Cibernética. O primeiro documento possui finalidade de orientar as atividades de defesa cibernética no nível estratégico, operacional e tático, supervisionadas pelo Ministério da Defesa (MD) (MINISTÉRIO DA DEFESA, 2012b). Os principais objetivos

traçados por essa política que merecem destaque são: assegurar o uso efetivo do ciberespaço pelas Forças Armadas (FA) do Brasil; capacitar recursos humanos para a condução das atividades no âmbito do MD; guiar a formulação de legislação e normas para o setor cibernético, contribuir com a produção de conhecimento cibernético e adequar as estruturas de CT&I das Forças Armadas (MINISTÉRIO DA DEFESA, 2012b).

O documento funciona como uma espécie de plano de ação na área de defesa cibernética, em que são apontadas as medidas consideradas cruciais para que o trabalho e a capacidade de atuação das FA no espaço cibernético sejam aperfeiçoados. As diretrizes analisadas como de maior importância no Livro Verde e que foram citadas anteriormente, aparecem também na Política Cibernética de Defesa (2012), o que reforça a relevância desses fatores para a defesa e a segurança cibernética do país.

O estabelecimento de projetos que fortaleçam a operacionalidade de comando e controle no MD, como a implantação do Sistema Militar de Defesa Cibernética (SMDC), a inclusão do conteúdo de defesa cibernética nos currículos dos cursos ministrados pelo MD, o estabelecimento de um canal técnico entre o SMDC e órgãos de Inteligência das Forças Armadas e a criação de parcerias entre centros militares de pesquisa e centros de pesquisa civis - públicos e privados - são algumas das diretrizes propostas no documento (MINISTÉRIO DA DEFESA, 2012b). Interpreta-se, portanto, que há a visão por parte do governo federal e do Ministério da Defesa de que existe uma carência de mecanismos técnicos institucionais para lidar com a defesa cibernética no país. A urgência do tema gera a necessidade de uma reformulação nas estruturas militares, para que se adequem ao contexto das ameaças trazidas pelo ciberespaço.

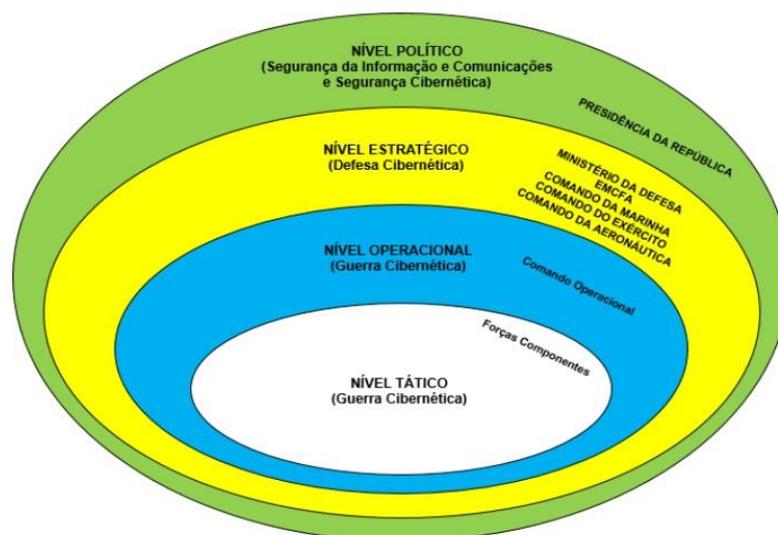
Além disso, o fator humano e o desenvolvimento tecnológico são elencados nas diretivas da Política Cibernética de Defesa (2012). A qualificação de talentos humanos perpassa pela definição de perfis do pessoal necessário para lidar com as atividades cibernéticas, bem como a criação de cargos e funções específicas e maior participação de profissionais do setor cibernético em áreas de estudos e especializações dentro e fora do país, em conjunto com uma campanha nacional de educação sobre defesa cibernética (MINISTÉRIO DA DEFESA, 2012b).

A questão tecnológica colocada em pauta preza pelo planejamento e execução da adequação das estruturas de CT&I com a integração de esforços entre as FA no setor cibernético, pela identificação das capacidades científico-tecnológicas necessárias ao desenvolvimento cibernético e pela criação de programas com característica dual (emprego civil e militar) para fortalecer o envolvimento do setor industrial na área cibernética (MINISTÉRIO DA DEFESA, 2012b). Por fim, o documento atenta para a elaboração de

normas e leis que guiem a aplicabilidade do ciberespaço no país, estabelecendo como um dos seus objetivos a realização de propostas de formulação e adequação de legislação federal que ampare as atividades de defesa cibernética no Brasil (MINISTÉRIO DA DEFESA, 2012b).

Já a Doutrina Militar de Defesa Cibernética (2014) possui como finalidade “estabelecer os fundamentos da Doutrina Militar de Defesa Cibernética, proporcionando unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa, e contribuindo para a atuação conjunta das Forças Armadas na defesa do Brasil no espaço cibernético” (MINISTÉRIO DA DEFESA, 2014, p. 13). O documento define os campos de atuação no setor cibernético e os seus respectivos órgãos/instituições responsáveis. A segurança cibernética fica a cargo da Presidência da República, por meio do GSI enquanto que a defesa cibernética fica a cargo do Ministério da Defesa, por meio das FA (MINISTÉRIO DA DEFESA, 2014).

Nessa divisão de atuações, fica estabelecido o nível de decisão de ações no contexto do ciberespaço. Primeiro, o nível político, que concentra a SIC e a segurança cibernética, coordenadas pela Presidência da República, abrangendo a Administração Pública Federal. A SIC é definida como “ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações” (MINISTÉRIO DA DEFESA, 2014, p. 19) O segundo nível, denominado de estratégico, compete às ações na área de defesa cibernética, orquestradas pelo MD, por meio do Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas. Por fim, os últimos são os níveis operacional e tático, que lidam com a guerra cibernética e ficam a cargo restrito das FA (MINISTÉRIO DA DEFESA, 2014).

Figura 2 - Organograma dos níveis de comando

Fonte: Ministério da Defesa (2014)

A Doutrina (2014) possui um caráter voltado totalmente ao setor militar, sendo caracterizada por conceituar os principais termos referentes ao espaço cibernético, expressando o entendimento do governo brasileiro sobre eles. Nessas conceituações, há o reconhecimento do ciberespaço como um dos cinco domínios operacionais, com a característica de permear todos os demais, visto que as atividades no espaço cibernético podem criar liberdade de ação para atividades em outros domínios (MINISTÉRIO DA DEFESA, 2014).

A defesa cibernética, por exemplo, fica definida como:

> [...] conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os sistemas de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (MINISTÉRIO DA DEFESA, 2014, p. 18).

É o primeiro documento brasileiro que declara o uso ofensivo de capacidades cibernéticas para o fim da defesa, assumindo, de maneira semelhante aos Estados Unidos, o possível uso do ciberespaço como um ambiente de projeção de poder. Poder este, definido no documento como a “capacidade de utilizar o espaço cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder” (MINISTÉRIO DA DEFESA, 2014, p. 19). Dentro desse contexto, os tipos de ações cibernéticas considerados pela Doutrina (2014) como capazes de afetar o ciberespaço e inferir no poder cibernético são os ataques cibernéticos, a proteção cibernética e a exploração cibernética, todos possuindo limites de atuação devido às suas capacidades e/ou constrangimentos externos, como atos normativos (MINISTÉRIO DA DEFESA, 2014).

Para a realização eficaz dessas ações, é posto a necessidade da coordenação entre as agências militares e civis. Essa coordenação traz o elemento da cooperação e do intercâmbio de informações como fatores essenciais, realçando que seja feito o fortalecimento de parcerias estratégicas entre os órgãos de segurança e defesa cibernética (MINISTÉRIO DA DEFESA, 2014). Dessa forma, mesmo o documento ser direcionado ao setor militar, considera impraticável o cumprimento da defesa cibernética e, consequentemente, da defesa nacional, sem o comprometimento de toda a sociedade brasileira em assumir responsabilidades, principalmente no caso das infraestruturas críticas que se utilizam do espaço cibernético (MINISTÉRIO DA DEFESA, 2014).

Infraestruturas críticas, na concepção brasileira, são “instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade” (MINISTÉRIO DA DEFESA, 2014, p. 19). A priorização pela defesa dessas

infraestruturas consta em todos os documentos oficiais do Brasil analisados, inclusive na Estratégia de Segurança da Informação e Comunicação e de Segurança Cibernética da Administração Pública Federal 2015-2018 (2015), que apresenta pela primeira vez orientações para que a proteção delas seja eficiente.

Apesar de ser um documento com prazo de validade e ela já ter vencido, é a primeira estratégia de segurança cibernética elaborada pelo governo federal que orienta os responsáveis pelas infraestruturas críticas do país a realizar: “(i) mapeamento de seus ativos de informação para a identificação daquele que são críticos; (ii) gestão de risco, com identificação de potenciais ameaças e vulnerabilidades; e (iii) estabelecimento de método de geração de alerta de segurança das infraestruturas críticas da informação” (GSI, 2015, p 53). As orientações indicam que as instituições responsáveis pelas infraestruturas críticas devem planejar e investir os recursos necessários para o fortalecimento das suas seguranças cibernéticas. Consequentemente, a interação entre órgãos da Administração Pública Federal e instituições públicas e privadas envolvidas no funcionamento das infraestruturas críticas é posto como quesito fundamental para que o Estado atue de modo efetivo na segurança cibernética do país (GSI, 2015).

Esse documento estabelece uma lista com diversas metas que deveriam ser cumpridas até o ano de 2018, como por exemplo, a promoção de uma conferência bianual de SIC e segurança cibernética da Administração Pública Federal e a proposição de métodos de identificação de ameaças e geração de alertas das infraestruturas críticas da informação (GSI, 2015). Entretanto, observa-se que muitas dessas metas não conseguiram ser alcançadas no país, entre elas os dois exemplos citados. Dois anos mais tarde, em fevereiro de 2020, o governo brasileiro publicou, por meio do decreto presidencial nº 10.222, a Estratégia Nacional de Segurança Cibernética – E-Ciber (2020), no intuito de resgatar alguns pontos da estratégia vencida em 2018 e aprimorar as discussões sobre o tema em nível nacional, estabelecendo diretrizes que terão validade no quadriênio 2020-2023.

Os três objetivos principais apresentados na estratégia são: tornar o Brasil mais próspero e confiável no ambiente digital, aumentar a resiliência brasileira às ameaças cibernéticas e fortalecer a atuação brasileira em segurança cibernética no cenário internacional (BRASIL, 2020). De maneira muito semelhante aos documentos oficias anteriores, a nova estratégia cibernética nacional do Brasil expressa os seguintes aspectos considerados cruciais para atingir os objetivos determinados: ampliar e promover um ambiente colaborativo entre o setor público, privado e a academia; elevar a proteção das infraestruturas críticas; aprimorar o arcabouço legal

do país sobre cibersegurança; incentivar a inovação tecnológica; ampliar a cooperação internacional e elevar o nível de maturidade da sociedade sobre o tema (BRASIL, 2020).

A parceria público-privado e academia visa estimular o compartilhamento de informações e a manutenção de um ambiente colaborativo que possibilite o estudo e a realização de exercícios cibernético em conjunto pelos atores. Essa ampliação cooperativa visualiza a colaboração do setor produtivo com a academia, por meio de recursos financeiros e materiais, que resulte tanto em um fomento de pesquisas no setor cibernético quanto uma maior utilização de tecnologias emergentes por parte do setor produtivo (BRASI, 2020).

Esse raciocínio converge com a estratégia de promover o desenvolvimento tecnológico no país. Pois, o incentivo a novos projetos acadêmicos em alinhamento com as necessidades da área produtiva busca encontrar inovações aos produtos nacionais que representem efeitos e soluções benéficas para a segurança cibernética. Por conseguinte, o documento estimula a criação de *startups* na área de segurança cibernética, urge para que investimentos em pesquisa sejam feitos e instiga a criação de centros de pesquisa e desenvolvimento no setor cibernético no âmbito do poder público e no setor privado (BRASIL, 2020).

Para que isso possa ser posto em prática, o capital humano aparece como recurso indispensável. O documento esclarece que a falta de cultura e conhecimento sobre o mundo digital e o espaço cibernético mostra que a sociedade brasileira ainda não está preparada para o uso adequado de ferramentas e tecnologias digitais. Como consequência, a alfabetização digital é tida como a saída para que a população tenha as habilidades necessárias para viver, aprender e trabalhar em uma sociedade da informação (BRASIL, 2020). As iniciativas identificadas são incentivar órgãos públicos e privados para a realização de campanhas publicitárias de conscientização e propor a inclusão do tema segurança cibernética na educação básica e superior do Brasil (BRASIL, 2020).

O desenvolvimento tecnológico também possui ligação com o desejo pela proteção eficiente das infraestruturas críticas do país. A estratégia almeja proporcionar maior resiliência às infraestruturas críticas, para que as atividades e os serviços essenciais continuem a serem executados mesmo em momentos de adversidades. Para atingir tal finalidade, de maneira distinta à Estratégia 2015-2018, as ações previstas consistem em:

> [...] promover a interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à segurança cibernética; estimular a adoção de ações de segurança cibernética pelas infraestruturas críticas; e incentivar que essas organizações implementem políticas de segurança cibernética, que contemplem, dentre outros aspectos, mecanismos de avaliação e de revisão periódica (BRASIL, 2020, n.p).

Em relação aos demais aspectos cruciais, mais uma vez é dado ênfase à cooperação internacional em segurança cibernética, buscando medidas estratégicas como uma ampliação de parcerias com o maior número possível de países, buscando a promoção de discussões sobre cibersegurança nos organismos, fóruns, eventos e exercícios internacionais no âmbito cibernético (BRASIL, 2020). O ciberespaço é visto como um assunto global e requer a interação entre atores internacionais para a construção de um ambiente digital seguro. O governo brasileiro se mostra disposto a adotar medidas de transparência, compartilhamento de informações e reafirmação da paz internacional, pois analisa que medidas globais irão contribuir para a viabilidade de requisitos mínimos de segurança cibernética no país para o uso de tecnologias avançadas, como o 5G. (BRASIL, 2020).

No último ponto de destaque, é elucidado que o Brasil precisa aprimorar o seu arcabouço legal no que se refere ao espaço cibernético. O governo admite que há a necessidade de revisar e atualizar os normativos existentes, abordar novas temáticas e elaborar novos instrumentos, principalmente devido aos dispositivos legais atuais não comtemplarem o setor produtivo, que abrange grande parte dos fornecedores de serviços essenciais. Nesse sentido, as ações apresentadas resumem-se em identificar e abordar temas ausentes na legislação vigente, incluir novas tipificações de crimes cibernéticos e formular normativos sobre tecnologias emergentes (BRASIL, 2020).

A Estratégia Nacional de Segurança Cibernética E-Ciber (2020) conclui trazendo a compreensão de que para que todos os pontos mencionados sejam implementados de maneira eficaz e efetiva, uma governança na área cibernética deve ser estabelecida no país. Relacionada às ações, mecanismos e medidas a serem adotadas com a finalidade de simplificar e modernizar a gestão dos recursos humanos, financeiros e materiais no setor (BRASIL, 2020). O documento menciona que um modelo mais centralizado de governança em segurança cibernética já é aplicado em países como os Estados Unidos e o Reino Unido, demonstrando que estruturas centrais que possuem autoridade para a condução do tema, estabelecendo regulamentos e ações específicas, apresentam bons resultados na coordenação e consolidação da segurança cibernética pelo Estado (BRASIL, 2020).

Nessa perspectiva, o GSI é visto como o órgão que deve exercer o papel central de coordenador estratégico, alinhando as ações nacionais de segurança cibernética a serem tomadas. A justificativa para o estabelecimento dessa governança está no grande e constante número de ataques e crimes cibernéticos que o Brasil vem recebendo nos últimos anos. É citado o relatório da *Internet Organised Crime Threat Assessment* (2018), que indica que o Brasil é alvo de 54% dos crimes e ataques no espaço cibernético ocorridos na América Latina, ocupando

o posto de primeiro lugar na região (BRASIL, 2020). Isso gera grandes prejuízos econômicos ao país. O documento utiliza como referência o *Norton Cyber Security Insights Report* (2017) que indica que o Brasil foi o segundo país no mundo com maior prejuízo devido à ataques cibernéticos no ano de 2017, no valor de US$ 22.5 bilhões. Dessa forma, a governança visa mitigar esses danos ao incorporar padrões de condutas em segurança cibernética.

Por fim, em setembro de 2020 entrou em vigor a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709 promulgada em 2018. É a primeira legislação que regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil. A nova lei possui o objetivo de assegurar o direito à privacidade e à proteção de dados pessoais e sensíveis dos usuários, estabelecendo regras sobre o tratamento desses dados por parte dos controladores e operadores no país. Os dados pessoais são definidos como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018, n.p) e os dados sensíveis como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018, n.p).

A LGPD não trata especificamente sobre uma estratégia cibernética, mas refere-se a medidas que devem ser tomadas tanto pelo Poder Público quanto pelo setor privado na segurança e proteção de informações individuais dos brasileiros. Fica determinado, por exemplo, que o tratamento de dados pessoais só pode ser realizado com o consentimento do titular desses dados, pessoa física ou jurídica (BRASIL, 2018). Além disso, o titular possui o direito ao acesso facilitado sobre o tratamento dos seus dados, que deve ser disponibilizada de forma clara pelo controlador, podendo o titular requisitar a correção, bloqueio ou eliminação de seus dados pessoais (BRASIL, 2018).

Ademais, a lei contém dispositivos que preveem as obrigações dos controladores e operadores de dados no Brasil, ficando submetidos à produção de relatórios que informe sobre a garantia da segurança das informações e dados e demonstre as operações de tratamento de dados (BRASIL, 2018). O controlador ou o operador que violar algum dos dispositivos e causar dano patrimonial ou moral, individual ou coletivo, por exemplo, pode sofrer sanções administrativas, como multa diária no valor limite de R$ 50 milhões (BRASIL, 2018). De modo geral, a LGPD estabelece regras de boas práticas sobre o tratamento e uso de dados e informações pessoais, levando em consideração a importância da proteção e segurança desses dados na garantia dos direitos fundamentais dos cidadãos e no desenvolvimento tecnológico do país.

Tabela 2 - Documentos governamentais brasileiros analisados

Documento	Data	Órgão responsável
Política Nacional de Defesa e Estratégia Nacional de Defesa	2012	Ministério da Defesa
Livro Verde: Segurança Cibernética no Brasil	2010	Gabinete de Segurança Institucional (GSI)
Livro Branco de Defesa Nacional	2012	Presidência da República
Política Cibernética de Defesa	2012	Ministério da Defesa
Doutrina Militar de Defesa Cibernética	2014	Ministério da Defesa
Manual Básico: Elementos Fundamentais	2014	Escola Superior de Guerra
Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018	2015	Gabinete de Segurança Institucional (GSI)
Lei Geral de Proteção de Dados	2018	Presidência da República
Estratégia Nacional de Segurança Cibernética	2020	Decreto Presidencial

Fonte: elaborado pelo autor

4.2 Discussão sobre as estratégias cibernéticas nacionais: aproximações e divergências

A percepção do governo brasileiro quanto à relevância do espaço cibernético na defesa nacional a partir da PND/END (2012) surgiu relativamente cedo, em um intervalo de tempo que pode ser considerado curto em relação às primeiras publicações das potências cibernéticas apresentadas. Entretanto, a maneira como cada país lidou com o assunto após a sua própria percepção vir a público ocorreu de modo distinto. O Brasil adotou uma abordagem de orientações e recomendações sobre o setor cibernético, sem firmar políticas públicas, estratégias e regulamentos legais de longo prazo à nível nacional para o setor. O caráter no qual o governo brasileiro tratou o tema foi de diagnóstico e identificação sobre os desafios que o ciberespaço trouxe, indicando caminhos pelos quais o Brasil pode enfrentá-los.

Essas indicações, apesar de extremamente úteis, acabam não sendo implementadas quando não há um arcabouço institucional e legal forte, já que o próprio Estado brasileiro reconhece a fragilidade da legislação vigente. O CDCiber, por exemplo, não tem função

regulamentar e suas iniciativas possuem pouca influência fora do ambiente militar (DA CRUZ, 2013). Dessa forma, o setor cibernético no país fica apenas sendo referido como um setor estratégico para a defesa e a segurança nacional, reconhecido por ser essencial na realização e coordenação de operações militares, mas o seu aprimoramento e desenvolvimento efetivo acaba não sendo sentido pela sociedade.

No Brasil, portanto, a cibersegurança pode ser considerada institucionalizada, mas compreendida como uma ampla atividade que está sob a alçada da Presidência, na qual está em um processo de securitização, pois ainda não possui reconhecimento do grande público, ao contrário de países como os EUA, que já se encontra em um processo consolidado, no qual o âmbito cibernético influencia as práticas governamentais, servindo de justificativa para o aprimoramento de mecanismos de vigilância, por exemplo (LOBATO; KENKEL, 2015). Pode se interpretar, ainda, que a proteção do ciberespaço é tratada de maneira menos urgente em países que são menos dependentes em sistemas de informação - países menos digitalizados - em que ameaças cibernéticas de proporções catastróficas são apenas especulações e adivinhações, e não uma realidade (LOBATO; KENKEL, 2015).

As principais diferenças observadas entre o Brasil e as potências cibernéticas, por conseguinte, se encontra na baixa digitalização do país latino americano e na ausência de uma estratégia cibernética brasileira de longo prazo, que preveja os programas, projetos e os planos de ações a serem implementados. Ou seja, observa-se a necessidade de uma estratégia de Estado para a defesa e a segurança cibernética no Brasil, e não somente estratégias de governo como foram as apresentadas até o atual momento, que possuem validade de tempo pré-determinadas e, por isso, não conseguem cumprir na prática com as suas metas e objetivos. O único documento que apresenta um projeto de longo prazo é o Livro Branco, porém, estabelece apenas ações de curto prazo e, assim como a PND/END e o Livro Verde, não trata sobre a implementação e aplicação efetiva das diretrizes determinadas, mas apenas das diretrizes em si.

Além disso, o baixo nível tecnológico e digital contribui para uma dependência tecnológica em relação a produtos importados de países com elevado grau de desenvolvimento em tecnologias da informação e comunicação. Dependência que dificilmente será superada sem a implementação de uma estratégia de longo prazo e grande alcance nacional (SOUZA; STREIT, 2017).

No sentido prático, muito do aprimoramento das capacidades cibernéticas no país foi devido aos eventos de grande magnitude ocorridos no país sul americano na última década, que tiveram grande contribuição para impulsionar a execução de ações de defesa e segurança no ciberespaço. Na Copa do Mundo de 2014, por exemplo, foi criado um centro para gerenciar o

tráfego de dados na rede e interromper movimentações suspeitas em cada cidade-sede do país (DOS SANTOS, 2019). Já nos Jogos Olímpicos de 2016, realizados no Rio de Janeiro, o Brasil contou com cerca de 200 especialistas, militares e técnicos atuando na proteção cibernética, aproximadamente o dobro do contabilizado na Copa do Mundo, dois anos antes (DOS SANTOS, 2019). A importância dos eventos refletiu na urgência de fortalecer as medidas de defesa e segurança cibernética, pois um hipotético blecaute nas cerimônias de aberturas ou uma falha no sistema de vendas de ingressos, por exemplo, resultariam em um verdadeiro desastre que mancharia a reputação internacional do país.

Dito isso, destaca-se as aproximações e distanciamentos entre o Brasil e os outros três países analisados no que se refere aos seus entendimentos sobre o espaço cibernético e as suas implicações para a defesa e a segurança nacional. Primeiro, entre os pontos de divergência, temos a pouca ênfase dada pelo governo brasileiro em relação à guerra cibernética, analisada apenas no espectro dos níveis táticos e operacionais. A política e a posição pacífica histórica do Brasil pode ser uma das justificativas para os documentos oficiais de defesa cibernética não tratarem sobre o tema de maneira mais acentuada. Diferentemente, as três potencias cibernéticas trazem o elemento da guerra como um propulsor das medidas de desenvolvimento das suas capacidades cibernéticas.

No caso da China, o pensamento estratégico segue uma linha de raciocínio com raízes na lógica de Chairman Mao, que acreditava que o caminho para quebrar o monopólio nuclear das superpotências e evitar uma possível coerção era desenvolver as próprias capacidades nucleares chinesas. Tal raciocínio pode ser atribuído às atitudes da China acerca do desenvolvimento de suas capacidades cibernéticas para a guerra atualmente (JIANG, 2019). O *cyberwarfare* ou a guerra cibernética, também é atrativo para os Estados Unidos, visto que podem utilizar o ciberespaço para robustecer o seu poder militar e/ou expandir as suas opções no que se refere à ações encobertas que o espaço cibernético possibilita (LINDSAY et al., 2015 *apud* JIANG, 2019).

Como visto no segundo capítulo, os EUA destacam a utilização ofensiva dos seus recursos cibernéticos, esclarecendo que fará uso das capacidades como armas cibernéticas através do ciberespaço. A maneira incisiva na qual aborda o assunto reflete o desejo estadunidense de garantir a sua vitória em qualquer guerra. Dessa forma, autoras como Healey (2013), acredita que mais operações ofensivas no setor cibernético serão realizadas pelo país, principalmente em vista da crença de que uma defesa cibernética ativa, que concentra mais formas de retaliação, é mais efetiva, devido às opções atrativas e de baixo custo que as capacidades cibernéticas ofensivas dispõem.

O Estado de Israel, principalmente devido ao contexto geopolítico regional no qual está inserido, também adota uma postura de constante aprimoramento de suas performances no campo de batalha e de suas capacidades em lutar guerras (BARAM, 2017). E o setor cibernético é tido como vital nesse sentido, dado que o governo israelense aparece na linha de frente no uso de tecnologias cibernéticas contra as ameaças que o país enfrenta em todas as áreas de um conflito (BARAM, 2017).

Além disso, no âmbito multilateral, a visão de Israel possui similaridade com a abordagem estadunidense, apesar da cooperação internacional ser um ponto pouco explorado nos documentos israelenses. Em 2016, Israel e Estados Unidos firmaram uma declaração de defesa cibernética de conectividade operacional em tempo real por meio dos seus respectivos CERTs (ADAMSKY, 2017).

O país do Oriente Médio enxerga o seu alto aperfeiçoamento cibernético como um atributo positivo para efetivar colaborações com outros países. O atual primeiro ministro do país, Benjamin Netanyahu, por exemplo, considera a cibernética como uma comódite, em que as soluções de segurança cibernética de Israel podem ser benéficas para os seus vizinhos, sendo um dos países pioneiros a introduzir a questão cibernética na esfera diplomática como um instrumento de *soft power* (ADAMSKY, 2017). O Brasil, por sua vez, expressa na sua Doutrina Militar (2014) o entendimento de que operações ofensivas destinadas a projetar poder através do espaço cibernético são uma realidade no cenário internacional. Entretanto, enfatiza que essas ações ofensivas ocorreriam apenas para manter a integridade da defesa nacional, e não como forma de projeção de poder.

Nesse sentido, pode se dizer que as ambições internacionais do Brasil diferem das potências analisadas, apesar de concordar com todas quanto ao estímulo à cooperação bilateral e multilateral como forma de avançar a defesa e a segurança cibernética no mundo. Nesse ponto, observa-se uma aproximação brasileira com a visão chinesa de cooperação internacional, principalmente dado o histórico da participação brasileira em fóruns internacionais.

Essa aproximação se fortaleceu após o vazamento de informações confidenciais por Edward Snowden, em 2013, no qual dentre os documentos vazados, ficou evidenciado uma espionagem estadunidense contra diversos países, incluindo o Brasil, que passaram a questionar o papel dominante dos EUA no ciberespaço global (SHEN, 2016). De maneira geral, houve uma maior coordenação entre os países do BRICS, apesar de não haver um completo consenso entre os membros em relação a algumas questões, como por exemplo, a soberania de dados (POLATIN-REUBEN; WRIGHT, 2014).

Uma das reações ao acontecimento de 2013, como uma tentativa de explorar soluções políticas conjuntas, foi a conferência NETmundial realizada no Brasil no ano de 2014, que consistiu em um encontro entre representantes da sociedade civil, academia e setor privado, em conjunto com 97 nações, com foco em propostas para a construção da governança da internet. Nela, China e Brasil concordaram com a aprovação do documento final que declarou que a governança da internet deveria ser construída em um processo democrático e com a participação de várias partes interessadas (HUANG; MACÁK 2017). Outra reação que, de certa forma, distanciou o Brasil da concepção estadunidense sobre o ciberespaço global foi a submissão, em conjunto com a Alemanha, da resolução "Direito à Privacidade na Era Digital*"*, em novembro de 2013, que abordou a soberania de dados como uma questão de direitos humanos, referente à violação da privacidade exposta pela vigilância em massa praticada (POLATIN-REUBEN; WRIGHT, 2014).

O rumo tomado pelo governo brasileiro frente aos vazamentos de Snowden, entretanto, não foi alinhado de modo absoluto com a visão chinesa frente ao cenário internacional. A ideia de soberania da informação pregado pelo governo chinês, tanto nos fóruns multilaterais quanto em seus documentos estratégicos, não é vista nos documentos e declarações do Brasil. A justificativa da China para tal postura parte do comportamento dos EUA perante o espaço cibernético, em que o governo chinês acredita ser necessário empregar a noção de soberania cibernética a fim de se proteger da influência ocidental (CUIHONG, 2018). Essa ideia reativa passa pelo fato de os Estados Unidos serem a potência dominante no ciberespaço global, devido ao seu papel na formação e no desenvolvimento da internet, além de ser o país que mais se beneficia economicamente com a internet global (AKDAG, 2019).

A ICANN, sediada na Califórnia, é um exemplo prático disso, pois apesar de ser um ator privado, responsável pela estrutura que regula o uso do DNS na internet global, teve na sua construção o apoio do governo estadunidense e, por muito tempo, uma dependência institucional direta com o Departamento de Comércio do governo estadunidense (DATYSGELD, 2017). Dessa forma, a crítica de nações como a China se concentra na influência, direta ou indireta, que os interesses estadunidenses têm sobre a ICANN, mesmo que tanto a organização quanto o governo dos Estados Unidos neguem essa vinculação. Atitudes chinesas, como o Grande Firewall da China, que bloqueia o acesso a determinados recursos e o tráfego de certas palavras chaves na internet, por exemplo, podem ser vistas como respostas do governo chinês com o intuito de preservar as ideologias e os valores nos quais o seu governo é legitimado, pois vê a natureza transnacional da internet como permissiva à invasão de ideias ocidentais (ZENG, 2017).

Outro ponto divergente do modelo cibernético brasileiro em relação às potências consiste na falta de políticas e diretrizes que configurem um processo de governança com arranjos formais e institucionais, capazes de estruturar as interações dos atores que participam ativamente da segurança cibernética do Brasil. Isso impacta como um desafio para o país, uma vez que resulta em uma baixa colaboração entre os atores do governo e do setor privado na formulação de políticas para a área (HUREL; LOBATO, 2018). A relação público-privado fica, por conseguinte, debilitada, por não ter bases que guiem a parceria entre os setores.

O setor privado, maior fornecedor de serviços, ferramentas e equipamentos cibernéticos acaba não recebendo o incentivo necessário para aperfeiçoar as suas atividades, visto que o poder público não oferece um rumo estratégico a ser seguido. "O maior desafio para uma governança multissetorial de segurança cibernética consiste na definição dos papéis e responsabilidades para cada setor" (HUREL; LOBATO, 2018, p. 4). Dessa forma, a análise de como funciona a parceria público-privado no Brasil se torna limitada, restando apenas a interpretação de que o aspecto é compreendido como relevante para o governo federal, já que é citado em diversos documentos oficiais brasileiros referentes à defesa e segurança cibernética.

Diferente do Brasil, as potências cibernéticas analisadas deliberam sobre as responsabilidades e funções que cada setor possui para garantir a efetividade da segurança cibernética em suas nações, estabelecendo diretrizes que visam estimular a relação público-privado. Nos Estados Unidos e em Israel, essa parceria ocorre principalmente por meio da determinação de políticas públicas que encorajam as empresas privadas a produzirem e a prestarem os seus serviços em áreas nas quais o governo considera essenciais para a construção de um ciberespaço seguro. Conforme esclarecido nos documentos oficiais, um dos meios utilizados na aprimoração dessa parceria é o compartilhamento de informações entre os setores.

Entre os exemplos práticos, ressalta-se o programa *Einstein,* nos EUA, fundamentado em um sistema de detecção de intrusões e tráfego de informações maliciosas que possuem como alvo redes civis do governo federal. Ele é coordenado pelo DHS e executado com a participação de prestadores de serviços comerciais. O programa coleta, correlaciona, analisa e compartilha dados e informações por toda a esfera federal, entre diversos setores, com a finalidade de aprimorar a consciência situacional em relação à segurança cibernética e as respostas contra as ameaças cibernéticas (PERNIK, 2016).

A intervenção do governo dos Estados Unidos na relação público-privado pode ser classificada como de promoção e suporte, defendendo o uso de certos padrões e estruturas para melhorar a compreensão dos atores, mas deixando a adoção das medidas para as entidades privadas (SPERL; THIA, 2017). Isso ocorre de modo similar no Estado de Israel, onde o

governo também se encarrega da responsabilidade de direcionar e aconselhar as empresas que provêm produtos e serviços cibernéticos. O exemplo prático de cooperação governamental com entidades privadas no caso israelense é a CERT, que promove o compartilhamento de informações e uma melhor coordenação entre as agências estatais e o setor privado contra ataques cibernéticos e na identificação de ameaças e vulnerabilidades cibernéticas (BENOLIEL, 2015).

Como foi visto, o objetivo estratégico de construir uma capacidade cibernética eficaz, exposto na Estratégia Nacional de Segurança Cibernética de Israel em Resumo (2017), visa proteger não só o sistema de redes do país, mas também os computadores e todo sistema de telecomunicação, através de meios que consigam identificar e prevenir ataques e incidentes. Nesse sentido, como exercício para a construção dessa capacidade cibernética, Israel criou unidades que contratam hackers para atentarem contra as próprias defesas cibernéticas de entidades públicas e privadas do país, como bancos, hospitais e serviços de abastecimento de água, com a finalidade de expor as suas potenciais vulnerabilidades e corrigi-las antes de realmente sofrerem um ataque (BERGMAN, 2012 *apud* COHEN, 2016).

A relação público-privado em Israel, portanto, perpassa por arranjos que instigam a inovação não apenas tecnológica, mas também de métodos. “A política de segurança cibernética de Israel tem procurado um modo de vida entre o governo e as corporações privadas, tentando equilibrar a eficiência de mercado, ciência e tecnologia, liberdades básicas e privacidade com a segurança de tecnologias da informação” (ADAMSKY, 2017, p. 115, tradução nossa)[69].

A China, no que lhe diz respeito, se distancia um pouco da perspectiva dos EUA e de Israel. O governo também funciona como o principal responsável por orquestrar a colaboração entre entes públicos e privados, mas em vista do caráter mais centralizado da forma de governo no país, essa relação é verticalizada, com os departamentos e agências estatais possuindo maior autoridade na condução das colaborações. Assim, a compreensão chinesa de que o país deve lutar pela soberania de seu ciberespaço para não sofrer influências ocidentais em seu ambiente interno pode ser visto como uma narrativa que reforça a legitimidade do governo em atuar de maneira direta na condução e supervisão das corporações privadas.

As obrigações estipuladas para os operadores de redes e de infraestruturas críticas na China, a partir dos documentos oficiais estudados, dão a dimensão de a relação púbico-privado no país funcionar a partir de um sistema de prestação de contas, em que o poder público

[69] Texto original: Israeli cyber security policy has been seeking a modus vivendi between the government and private corporations, trying to balance market efficiency, science and technology, basic freedoms, and privacy with IT security.

supervisiona e monitora os operadores e as entidades privadas. Há mais de 10 anos, por exemplo, a China iniciou um processo de implementar um sistema de nomes reais na rede, em que autoridades governamentais requisitam de provedores de serviços de internet, como cibercafés, que os usuários façam um registro fornecendo suas identidades e informações pessoais para que tenham acesso à internet (QI et al, 2018). Ou seja, em comparação com a relação entre o setor público e o setor privado que ocorre em Israel e nos EUA, o governo chinês demonstra ter maior intervenção e coordenação sobre as ações das empresas privadas, na condução dos seus processos produtivos e de fornecimento de serviços.

A convergência entre os quatro países no que se refere a parceria público-privado é a sua categorização como um meio estratégico para alcançar o objetivo do desenvolvimento e da inovação das suas capacidades tecnológicas, em especial as TICs. Para os Estados Unidos, o domínio de tecnologias de ponta contribui para a manutenção de um *status quo* no qual o país norte americano é o maior beneficiado, preservando a sua posição de potência mundial tanto no sentido econômico, por meio da economia digital, baseada em *e-commerce* e propriedade intelectual; quanto militar, por expandir e aprimorar as suas ferramentas de combate, aumentando a probabilidade de vencer conflitos e guerras.

Para Israel, contribui para manter o status de polo tecnológico mundial desejado pelo país e o fortalece em seu complexo regional, minando as constantes ameaças à defesa e a segurança nacional que recebe de seus adversários. Para a China, o aprimoramento de novas tecnologias propõe justamente confrontar o *status quo*, desafiando as visões ocidentais sobre o ciberespaço com o desejo de não permitir que influenciem ou perturbem a sociedade chinesa e os seus valores, assim como contribui para projetar o país a um alto nível de competitividade no mercado internacional.

Retornando ao Brasil, também há nos documentos brasileiros a identificação do desenvolvimento tecnológico e da parceria público-privado como fatores estratégicos, mas assim como não há a atribuição de funções e responsabilidades claras para os diferentes setores, a falta de uma estratégia cibernética de Estado para o setor cibernético também evidencia uma certa vagueza nos objetivos brasileiros em relação a esses elementos. Isso faz com que, no fim das contas, a aprimoração das capacidades cibernéticas do país fique refém de acontecimentos, como os eventos internacionais comentados, que de certa forma obrigam os atores públicos e privados a buscarem formas mais eficazes de executarem as suas atividades para salvaguardar a segurança nacional.

Para completar, dentre os pontos mais reincidentes e com maiores destaques nas publicações das quatro nações observadas, o fator humano é posto como peça fundamental na

engrenagem que move a defesa e a segurança cibernética. É inegável que tudo o que foi mencionado acima, desde os aspectos da cooperação internacional até o desenvolvimento tecnológico e a proteção das infraestruturas críticas, passa por um fator em comum: recursos humanos. É a humanidade quem constrói as estruturas e os mecanismos nos quais se apoia para continuar progredindo como espécie, bem como é quem destrói ou deixa de lado arranjos e disposições que considera não ser mais útil ou benéfico para o seu bem estar e progresso. Essa lógica também se aplica nos Estudos Estratégicos de Segurança e Defesa, pois os métodos, operações, táticas, equipamentos e serviços vão sendo aperfeiçoados ao longo do tempo graças ao capital humano que formula novas linhas de pensamento e as coloca em prática.

Dessa forma, não há como conceber novos órgãos institucionais de proteção contra ataques cibernéticos, por exemplo, ou realizar pesquisas científicas voltadas ao espaço cibernético e suas especificidades sem que haja indivíduos capacitados para conduzir essas atividades. As próprias TICs também são pensadas e produzidas por mãos humanas e de nada tem valor sem o uso social na qual possibilitam, pois ao mesmo tempo em que é o produtor, o indivíduo é também o usuário.

> Quanto aos parâmetros de usuários, observa-se que os mesmos são atores essenciais para o bom funcionamento do processo de implementação de qualquer iniciativa na área de segurança, pois se constata que este pode se tornar a parte mais vulnerável de todo o sistema de informação e comunicação (HOSANG, 2011, p. 13).

Dito isso, vemos que no Brasil a abordagem perante o fator humano e o envolvimento da sociedade civil como um todo é de assimilação, em que a sua importância é apenas introduzida e apresentada nos documentos. Consequentemente, o governo brasileiro assume que medidas devem ser tomadas, mas, mais uma vez, não apresenta planos de ações que orientem a execução prática dessas medidas. Dessa forma, o nível de expertise dentro da comunidade de inteligência no país, que é uma das bases para os mecanismos de defesa cibernética, está longe de alcançar o patamar necessário para confrontar as ameaças atuais (GONÇALVES, 2012 *apud* LOBATO; KENKEL, 2015).

Um exemplo disso é a ausência de uma agência de Inteligência de Sinais (SIGINT) no Brasil, cuja função é coletar as transmissões de dados e informações que podem ser feitos por intermédio de satélites, sistemas informáticos específicos, etc. (REIS, 2014). Mesmo com a recomendação do Senado Federal para a sua construção, após a CPI que investigou as denúncias feitas por Snowden e apontou que os orçamentos da área de inteligência e de defesa cibernética no Brasil são inferiores aos de suas contrapartes internacionais, a criação de tal agência não foi concretizada (MALAGUTTI, 2017).

A atividade de Inteligência parte de compreender e prever o comportamento humano e, por conseguinte, de determinado grupo e/ou governo, buscando conhecer nossas emoções, consciência e como funcionamos enquanto sociedade por meio da obtenção de informações (REIS, 2014).

> Uma agência de Inteligência governamental deve conhecer esse processo emocional do ser humano e se utilizar desse conhecimento para adquirir informação do outro e para ajudar os seus a se protegerem dos demais. Ou seja, o fator humano é primordial no jogo de poder existente na comunidade internacional (REIS, 2014, p. 8).

Além disso, também não há um projeto nacional para a formação e especialização de profissionais na área cibernética, especialmente civis. Os documentos brasileiros, como o decreto publicado em 2020, declaram a necessidade de incentivos estatais para que estudos sobre segurança cibernética e o ciberespaço, de modo geral, façam parte das disciplinas ofertadas em cursos superiores e da pesquisa acadêmica nacional. Porém, a atividade prática fomentada por incentivos e políticas públicas realizada no Brasil para o treinamento de especialistas se concentra no setor militar, especialmente voltada para a defesa cibernética. O Exercício Guardião Cibernético, como é denominado, consiste em um evento conduzido pelo Comando de Defesa Cibernética (ComdCiber) com a finalidade de treinar os participantes em proteção cibernética através do Simulador de Operações de Guerra Cibernética (SIMOC), em que os envolvidos devem tomar decisões e realizar exercícios para responder a eventos cibernéticos em tempo real (EXÉRCITO BRASILEIRO, 2019).

Ao se analisar as potências cibernéticas, vemos que nos EUA, por exemplo, a relevância do fator humano resultou na formulação e implementação de projetos de estudos e programas de conscientização da sociedade civil. O programa NICE é um dos exemplos, já citado no capítulo anterior, que almeja expandir e aprofundar o ensino sobre o espaço cibernético na academia norte americana e, consequentemente, aumentar o percentual de profissionais e especialistas no setor cibernético no país. O programa firma parcerias com organizações civis e provê oportunidades para indivíduos e grupos de indivíduos terem contato com assuntos cibernéticos e aperfeiçoarem as suas habilidades dentro do espaço cibernético (PAULSEN et al., 2012).

São formuladas parcerias com centros comunitários, escolas, faculdades e universidades por todo o país para promover os *Cyber Citizen Forums*, que ensinam conteúdos e treinamentos práticos sobre segurança cibernética (PAULSEN et al., 2012). Outro programa com enfoque em melhorar o capital humano iniciado em 2012 nos EUA é o *CyberSkills Task Force*, coordenado pelo DHS, em que entidades da indústria e do governo fornecem uma série de

recomendações a fim de desenvolver uma força de trabalho capacitada em cibersegurança (CONKLIN, 2014).

A consciência da população também é um debate levantado pela China, que, conforme visto, enxerga que fluxos de informações maliciosos podem prejudicar a sociedade e perturbá-la, vindo a corresponder como uma ameaça à soberania nacional. Nesse sentido, o fator humano é elevado a um patamar de máxima importância, dado que, na compreensão chinesa, o comportamento dos cidadãos chineses pode levar a uma instabilidade política e social na nação. "O governo chinês tem a preocupação de que o acesso irrestrito à internet ou a informações ou dissidências não controladas pode se tornar uma ferramenta de subversão e colocar uma ameaça significativa à segurança política chinesa" (CUIHONG, 2015, p.12, tradução nossa)[70].

A China não possui um sistema de programas nacionais baseado na integração entre governo, setor privado e academia tão sofisticado e que tenha servido como propulsor do conhecimento e do desenvolvimento da indústria de alta tecnologia como os Estados Unidos (AUSTIN, 2018). Entretanto, nos últimos anos o país tem conseguido produzir números muito próximos dos EUA na formação de PhDs, contabilizando todos os cursos disponíveis, incluindo cursos voltados ao setor cibernético. Em 2014, por exemplo, as universidades estadunidenses graduaram 54,070 novos doutores, enquanto que as universidades chinesas graduaram 52,654 no ano de 2015 (AUSTIN, 2018). No que diz respeito especificamente à segurança cibernética, no ano de 2016 a China contava com 122 universidades e faculdades com programas de mestrado, sendo que algumas possuíam também programas de especializações em cursos de segurança da informação e departamentos especializados em privacidade de dados, resultando no treinamento de aproximadamente 10,000 graduados por ano (ZHANG et al. 2016 *apud* AUSTIN, 2018).

Contudo, existe a expectativa de que isso não seja suficiente para suprir a demanda no mercado por profissionais na área cibernética no país, principalmente por ser uma área que exige uma alta diversidade de mão de obra, como engenheiros, cientistas da computação, programadores, desenvolvedores, entre outros. A China pode ter um déficit de força de trabalho em segurança cibernética de aproximadamente 1.4 milhão de profissionais no ano de 2020, de acordo com Feng Huaming, vice-presidente do *Beijing Institute of Eletronic Science and Technology Institue* (XINHUA, 2017). Além disso, as universidades chinesas, de modo geral, ainda não conseguem alcançar o mesmo nível em qualidade de pesquisa e impacto internacional que os seus pares ocidentais (SHUANG et al. 2016 *apud* AUSTIN, 2018).

[70] Texto original: The Chinese government worries that unrestricted Internet access or uncontrolled information or dissent might become a tool of subversion and pose a significant threat to Chinese political security.

Em Israel o foco do aperfeiçoamento dos recursos humanos se concentra especialmente na sofisticação de tecnologias através de inovações e desenvolvimento. Além das estruturas legais e as políticas feitas em relação ao estímulo na formação de profissionais, as políticas do governo israelense se concentram no estímulo à inovação através de mecanismos legais. Como o *The Encouragement of industrial research and development Law 5744-1984*, que encoraja companhias israelenses a investirem em projetos de pesquisa e desenvolvimento, com o governo assumindo os riscos inerentes aos projetos (TABANSKY; ISRAEL, 2015).

O investimento em pesquisa e desenvolvimento baseado em centros de pesquisa interdisciplinares em universidades de Israel, financiados pelo governo, é uma das facetas da política nacional cibernética do INCB (BENOLIEL, 2015). Ou seja, o comando cibernético do país se utiliza de uma lei de fomentos a inovações tecnológicas já existente desde 1984 para aplicar incentivos no ramo cibernético. Segundo Benoliel (2015), Israel segue as experiências dos Estados Unidos e do Reino Unido, se comprometendo a desenvolver as suas capacidades de segurança cibernética por dois motivos; primeiro para cultivar a dinamicidade das comunidades de pesquisa capazes de lidar com os desafios de segurança cibernética para as próximas gerações; e segundo, por esse comprometimento permitir que as indústrias nacionais de cibersegurança expandam e acessem mercados no exterior.

No que concerne à educação cibernética, o país do Oriente Médio possui iniciativas nacionais para instigar a compreensão pública sobre ameaças cibernéticas e para concentrar esforços na produção e desenvolvimento de talentos na área. O *IDF Unit 8200*, unidade do Corpo de Inteligência de Israel, por exemplo, atua como uma incubadora de tecnologias com foco em segurança cibernética, recrutando talentos em escolas e universidades ao redor do país (LEWIS, 2016). “Os tecnólogos da Unidade 8200 trabalham diretamente com seus clientes para desenvolver produtos inovadores e aprender habilidades iniciais cruciais. Os ex-alunos da unidade fundaram diversas empresas israelenses líderes” (LEWIS, 2016, p. 28, tradução nossa)[71]. O que se torna evidente, portanto, é a identificação do capital humano como fonte imprescindível na evolução dos mecanismos cibernéticos dos países em um âmbito geral e também na melhoria da eficiência dos Estados em lidar com as ameaças e vulnerabilidades cibernéticas.

De maneira geral, observa-se maiores aproximações e semelhanças entre as abordagens estadunidenses e israelenses no tratamento aplicado tanto em relação ao capital humano quanto em outros fatores que influenciam a segurança e a defesa cibernética de uma nação. A China,

[71] Texto original: Unit 8200’s technologists work directly with their customers to develop innovative products and learn critical startup skills. The unit’s alumni founded many leading israeli companies.

por sua vez, implementa suas ações com diferentes métodos, mas a partir das mesmas identificações, ilustrando que a raiz das divergências entre as três potências cibernéticas se concentram nas visões políticas que possuem não só sobre o assunto, mas sobre as formas de governança e como enxergam a política internacional e a segurança nacional.

No fim, a intersecção se encontra no entendimento técnico que têm sobre defesa e segurança cibernética, pois os diagnósticos são muito semelhantes, apenas as soluções necessariamente não são as mesmas. O Brasil se insere posteriormente e de modo defasado tecnologicamente no contexto cibernético, reconhecendo que ainda há muito o que fazer nessa área, principalmente no sentido das ações práticas e dos mecanismos legais. Mas a forma como o país sul americano apresenta as suas concepções perante o espaço cibernético não destoa de maneira substancial das concepções apresentadas por EUA, China e Israel. Interpreta-se, nesse sentido, que o governo brasileiro está seguindo um certo padrão na identificação dos fatores estratégicos e fundamentais nos quais uma nação precisa despender esforços para atingir um nível adequado de defesa e segurança cibernética.

Não é possível afirmar que há uma importação das ideias cibernéticas das grandes potências mundiais para o ambiente nacional do Brasil, nem mesmo para países periféricos em geral. Porém, fica evidente que a abordagem tanto dos Estados Unidos, China e Israel, quanto do Brasil, se assemelham na caracterização das questões consideradas como basilares na construção de um espaço cibernético seguro. As divergências se concentram no momento após essa caracterização e identificação, quando caminhos e direções são indicados para serem seguidos pelos atores que compõe a defesa e a segurança do ciberespaço.

5 CONCLUSÃO

As estratégias cibernéticas nacionais de EUA, China, Israel e Brasil categorizam o ciberespaço como um importante domínio de poder, demonstrando preocupações em relação ao uso e à participação direta desse novo ambiente não apenas nos conflitos atuais e do futuro, mas em todo o funcionamento e ordenamento da sociedade global. De modo geral, os quatro países abordam com seriedade a relevância da defesa e da segurança cibernética, identificando e apontando fatores estratégicos semelhantes para construir um espaço cibernético seguro. Fatores como a relação público-privado, a proteção das infraestruturas críticas, o desenvolvimento tecnológico, a capacitação de recursos humanos e a cooperação internacional são encontrados de maneira recorrente nos documentos governamentais oficiais dos países estudados, indicando uma correlação entre os modelos cibernéticos analisados.

Há uma convergência, portanto, na percepção dos elementos considerados estratégicos por cada um dos países. Entretanto, as abordagens adotadas após a identificação desses fatores apresentam certas divergências, especialmente devido ao entendimento político que cada país possui sobre o domínio cibernético. Em relação ao âmbito internacional, por exemplo, as quatro nações se mostram favoráveis à cooperação internacional e uma maior aproximação multilateral entre os países no setor cibernético. Contudo, a República Popular da China enxerga o ciberespaço como um espaço a ser territorializado, pois considera que o fluxo de informações em um ciberespaço global sem normas e regulamentos internacionais oficiais pode representar uma ameaça à sua soberania e estabilidade interna. Consequentemente, julga que os países deveriam trabalhar na construção de uma governança global da internet gerenciada pela ONU. Uma compreensão que difere da concepção estadunidense, que em nome da liberdade do trânsito de informações e dados acredita que a internet não deve ter uma entidade internacional reguladora, mantendo o gerenciamento dos protocolos e endereços de IP com a ICANN.

Sendo assim, a visão política que legitima a forma de governar em cada um dos países se mostra presente nos caminhos e direções das ações que devem ser implementadas no ciberespaço. Desse modo, interpreta-se que há certo padrão na identificação dos fatores que influenciam diretamente no cumprimento dos objetivos expostos nos documentos nacionais. A percepção estratégica das três potências cibernéticas analisadas, por exemplo, não possui grandes divergências quanto ao que deve ser feito para que a defesa e a segurança cibernética sejam garantidas em suas nações, mas sim em como deve ser feito. Ou seja, as divergências necessariamente não se encontram no reconhecimento dos fatores estratégicos para o espaço

cibernético, mas ocorrem após a sua identificação, quando é delineada a forma com que cada ação deve ser tomada.

A maneira de coordenar e lidar com a parceria entre o setor público e privado também é outro grande exemplo. Pois, apesar de as três potências cibernéticas estimularem tal parceira em suas estratégias, Israel e EUA buscam criar mecanismos de incentivos e medidas de suporte entre os setores, enquanto a China, além dos incentivos, estabelece instrumentos de supervisão e gerenciamento por parte das agências estatais perante as entidades privadas. Nesse contexto, interpreta-se que a as maiores aproximações da estratégia cibernética do Brasil com os países estrangeiros analisados se configuram justamente na caracterização dos fatores estratégicos citados. Os distanciamentos se concentram principalmente nas particularidades do Brasil, que por ser um país com baixo nível de desenvolvimento tecnológico na área cibernética, precisa focar no aprimoramento de questões já estabelecidas nos EUA, China e Israel, como a instituição de regulamentos oficiais estratégicos de longo prazo para o ciberespaço e o processo de digitalização do país.

A semelhança nos fatores estratégicos indica uma relação entre os modelos cibernéticos estrangeiros analisados e o modelo cibernético brasileiro. Em que por não haver uma regulamentação internacional, os países mais avançados e que foram pioneiros no estabelecimento de diretrizes e dispositivos para o ciberespaço, em especial a China e os EUA, acabam servindo de referência para o país sul-americano na construção de suas diretrizes para a defesa e a segurança cibernética. Contudo, não é possível confirmar a hipótese de que isso ocorre com os demais países periféricos no sistema internacional em vista do pequeno número de países analisados nesta pesquisa. A comparação de apenas um país tido como em desenvolvimento com três países desenvolvidos no âmbito cibernético não é suficiente para assumir generalizações. É preciso que mais pesquisas e trabalhos sejam realizados comparando mais países atrasados tecnologicamente e que não possuem estratégias cibernéticas bem consolidadas, com países considerados potências cibernéticas e que possuem estratégias bem definidas para o ciberespaço para que a hipótese possa ser atestada.

REFERÊNCIAS

ADAMSKY, Dmitry. **The Israeli Odyssey toward its National Cyber Security Strategy**. The Washington Quarterly, vol. 40, nº 2, p. 113-127, 2017. https://doi.org/10.1080/0163660X.2017.1328928.

AKDAG, Yavuz. **The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective**. Journal of Chinese Political Science/Association of Chinese Political Studies, nº 24, p. 225-247, 2019.

ARQUILLA, John; RONFELDT, David. **Cyberwar is Coming!** In: ARQUILLA, John; RONFELDT, David (Ed). **In Athena's Camp: Preparing for conflict in the Information Age**. Santa Monica, CA. Rand Publishing, 1997, p. 23-60. Disponível em: < https://www.rand.org/pubs/monograph_reports/MR880.html>. Acesso em: 10 de abril de 2020.

AUSTIN, Greg. **Cybersecurity in China: The Next Wave**. SpringerBriefs in Cybersecurity. Springer International Publishing, 2018. ISBN 978-3-319-68436-9 (eBook).

AYRES PINTO, D.J.; FREITAS, R.S., PAGLIARI, G. C. **Fronteiras virtuais: um debate sobre segurança e soberania do estado.** In.: AYRES PINTO, D.J, FREIRE, M.R., CHAVES, D. S. **Fronteiras Contemporâneas Comparada**: desenvolvimento, segurança e cidadania. Macapá: Editora da UNIFAP, 2018, p. 40-53.

BALDWIN, David A. **The concepto f security**. Review of International Studies, vol. 23, p. 5-23. 1997.

BARAM, Gil. **Israeli Defense in the Age of Cyber War**. Middle East Quaterly, vol. 24, nº 1. p. 1-10, 2017.

BENOLIEL, Daniel. **Toward a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study**. North Carolina Journal of Law & Technology, vol. 16 (3). Article 4, p. 435-486. Disponível em: < http://scholarship.law.unc.edu/ncjolt/vol16/iss3/4>. Acesso em: 3 de maio de 2020.

BENTO, Walfredo F. N. **Por uma Geopolítica Cibernética: apontamentos da Grande Estratégia brasileira para uma nova dimensão da guerra**. 2013. 212f. Dissertação de Mestrado. Universidade Federal Fluminense. Niterói, RJ. 2013.

BOBBIO, N.; MATTEUCCI, N.; PASQUINO, G. **Dicionário de Política**. Brasília: Editora Universidade de Brasília, 1998.

BRASIL. **Estratégia Nacional de Segurança Cibernética – E-Ciber**. Presidência da República. Brasília, Decreto nº 10.222, Brasil, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm>. Acesso em 2 de maio de 2020.

BRASIL. **Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018.** Presidência da República. Brasília, Brasil, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 23 de fevereiro de 2021.

BRASIL. **Livro Branco de Defesa Nacional**. Presidência da República, Ministério da Defesa. Brasil, Brasília, 2012. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 20 de março de 2021.

BRUNST, Phillip W. **Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet**. In: WADE, Marianne; MALJEVIC, Almir. **A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications**. Nova York: Springer Sciences+Busisness Media, 2010. p. 51-81.

BUEN, Ana T. **The Role of Cyberspace in Interstate Tensions and Conflicts**. 2016, 38f. Dissertação de Mestrado, Leiden University. Leiden. 2016.

BUZAN, Barry. **Rethinking Security after the Cold War**. Cooperation and Conflict. SAGE Publications. Vol. 32 (1). p. 5-28, 1997.

CARVALHO, Paulo S. M. **A Defesa Cibernética e as Infraestruturas Críticas Nacionais**. CMS, Núcleo de Estudos Estratégicos. Escola de Comando e Estado-Maior do Exército, Rio de Janeiro. 2011. Disponível em: < http://www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf>. Acesso em: 28 de jan. 2020.

CHANG, Amy. **Warring State: China's Cybersecurity Strategy**. Center for a New American Security, Washington, p. 1- 44, 2014.

CHINA. **Pareceres do Grupo de Liderança Nacional em Informatização sobre Fortalecimento da Segurança da Informação**. República Popular da China, Beijing, 2003. Disponível em: <https://www.tc260.org.cn/front/postDetail.html?id=20141211105253>. Acesso em: 26 de março de 2020.

CHUNG, Alex et al. **CiberSecurity: Policy**. In: L.R, Shapiro; M-H, Maras. **Encyclopedia of Security and Emergency Management**. Springer Nature Switzerland, p.1-9, 2019.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War: The Next threat to National Securtiy and What to Do About it**. Harper Collins Publisher, New York, 2010.

COHEN, Matthew S. et al. **Israel and Cyberspace: Unique Threat and Response**. International Studies Perspectives, p. 1-15, 2016, doi: 10.1093/isp/ekv023.

CONKLIN, Wm Arthur et al**. Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors**. 47th Hawaii International Conference on System Science. IEEE Computer Science. p. 2006-2014, 2014. DOI 10.1109/HICSS.2014.254.

COURIEL-HOUSEN, Deborah. **National Cyber Security Organisation: ISRAEL**. NATO CCD COE. Talinn, 2017. Disponível em: < https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf>. Acesso em: 29 de março de 2020.

CUIHONG, Cai. **Cybersecurity in Chinese Context: Changing Concepts, Vital Interests and Cooperative Willingness**. 9th Berlin Conference on Asian Security. German Institute for International and Security Affairs. Berlim, p. 1-25, 2015.

CUIHONG, Cai. **Global Cyber Governance: China's Contribution and Approach**. World Century Publishing Corporation and Shanghai Institutes for International Studies. China Quarterly of International Strategic Studies, vol. 4, nº 1, p. 55-76, 2018. DOI: 10.1142/S2377740018500069.

CYBERSPACE ADMINISTRATION OF CHINA. **Pareceres da Comissão Militar Central solicitando maior fortalecimento da segurança militar da informação**. República Popular da China, 2014. Disponível em: <www.cac.gov.cn/2014-10/08/c_1112729858.htm>. Acesso em: 21 de março de 2020.

CYBERSPACE ADMINISTRATION OF CHINA. **Estratégia Nacional para a Segurança no Ciberespaço**. República Popular da China, 2016. Disponível em: <www.cac.gov.cn/2016-12/27/c_1120195926.htm>. Acesso em: 23 de março de 2020.

DA CRUZ J. Samuel C. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Instituto de Pesquisa Econômica Aplicada (IPEA), nº 1850, p. 1-51, Brasília, 2013. Disponível em: < https://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_1850.pdf>. Acesso em: 1 de maio de 2020.

DATYSGELD, Mark W. **O papel da Governança da Internet dentro da Governança Global: Um estudo de caso da ICANN**. Pontifícia Universidade Católica de São Paulo (PUC-SP). Dissertação de Mestrado, 156f, São Paulo, 2017.

DE LAURA, Davey A. **United States Government CyberSecurity Policy: Protecting Critical Infrastructure from Malicious Hacker Attack Methods and CyberWar**. 2010. 155f. Dissertação de Mestrado. University of Hawai'i. Manoa, 2010.

DEPARTMENT OF DEFENSE. **DoD Dictionary of Military and Associated Terns**. Department of Defense, United States. Jan. 2020.

DEPARTMENT OF DEFENSE. **Resumo da Estratégia Cibernética**. Estados Unidos, 2018a. Disponível em: <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>. Acesso em: 2 de fevereiro de 2020.

DEPARTMENT OF DEFENSE. **Resumo da Estratégia de Defesa Nacional dos Estados Unidos da América**. Estados Unidos, 2018b. Disponível em: <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>. Acesso em: 19 de fevereiro de 2020.

DEPARTMENT OF DEFENSE. **Dicionário do Departamento de Defesa sobre Termos Militares e Associativos**. Department of Defense, Estados Unidos, 2020. Disponível em: < https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>. Acesso em: 10 de março de 2020.

DEPARTMENT OF HOMELAND SECURITY. **Plano Nacional de Proteção a Infraestrutura (NIPP)**. Estados Unidos, 2013. Disponível em: <https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf>. Acesso em: 17 de março de 2020.

DEPARTMENT OF HOMELAND SECURITY. **Estratégia de Segurança Cibernética do Departamento de Segurança Interna dos Estados Unidos**. Estados Unidos, 2018. Disponível em: <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf>. Acesso em: 2 de fevereiro de 2020.

DOS SANTOS, Bruno I. L. **O Emprego da Capacidade Cibernética nas Operações Militares em Grandes Eventos no Brasil: Emprego do Centro de Defesa Cibernética nos Jogos Olímpicos de 2016**. Escola de Aperfeiçoamento de Oficiais. Rio de Janeiro, p. 1-18, 2019. Disponível em: < https://bdex.eb.mil.br/jspui/bitstream/123456789/5382/1/Artigo%20Cienti%CC%81fico%20Bruno%20%C3%8Dgaro%20esao.pdf>. Acesso em 1 de maio de 2020.

EFTHYMIOPOULOS, Marios P. **A cyber-security framework for development, defense and innovation at NATO**. Journal of Innovation and Entrepreneurship. Vol. 8:12 (2019). https://doi.org/10.1186/s13731-019-0105-z.

EILSTRUP-SANGIOVANNI, Mette. **Why the World Needs an International Cyberwar Convention**. Philosophy Technology, vol 31, p. 379-407, 2018.

ESCOLA SUPERIOR DE GUERRA. **Manual Básico: Elementos Fundamentais**. Escola Superior de Guerra. vol. 4. Rio de Janeiro, Brasil. 2014.

EXÉRCITO BRASILEIRO. **Exercício Guardiao Cibernético 2.0**. Ministério da Defesa, Exército Brasileiro (EB), Brasil, 2019. Disponível em: < https://www.eb.mil.br/web/imprensa/aviso-de-pauta/-/asset_publisher/0004ie79MBVM/content/exercicio-guardiao-cibernetico-2-0#:~:text=A%20atividade%20envolve%20a%20prote%C3%A7%C3%A3o,de%20simula%C3%A7%C3%B5es%20virtual%20e%20construtiva.>. Acesso em: 22 de fevereiro de 2021.

FERREIRA, Juliana A.B. **A Questão Cibernética nas Relações entre os Estados: Uma Novas Forma de Projeção de Poder na Atualidade**. 2017. 121f. Dissertação de Mestrado, Universidade Federal Fluminense, Niterói, 2017.

GABINETE DE SEGURANÇA INSTITUCIONAL. **Livro Verde – Segurança Cibernética no Brasil**. Gabinete de Segurança Institucional da Presidência da República. Brasília, Brasil. 2010. Disponível em: <http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 26 de abril de 2020.

GABINETE DE SEGURANÇA INSTITUCIONAL. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018**. Presidência da República, Brasil, Brasília, 2015. Disponível em:

<https://www.gov.br/gsi/pt-br/arquivos/4_estrategia_de_sic.pdf>. Acesso em 1 de maio de 2020.

HADDAD, Christian; BINDER, Clemens. **Governing through cybersecurity: national policy strategies, globalized (in-)security and socioethnical visions of the digital Society**. Osterreich Z Soziol, vol. 44, p. 115-134, 2019.

HEALEY, Jason. **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. Cyber Conflict Studies Association (CCSA), 2013.

HERCHEUI, Magda et al. **ICT Critical Infraestructures and Society**. In: IFIP TC 9 International Conference on Human Choice and Computers, 10. ed. Amsterdam, Springer, 2012.

HUANG, Zhixiong; MACÁK, Kubo. **Towards the International Rule of Law in Cyberspace: Constrasting Chinese and Western Approaches**. Oxford University Press. The Chinese Journal of International Law, p. 271-310, 2017. doi:10.1093/chinesejil/jmx011.

HUREL, Louise Marie; LOBATO, Luisa C. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**. Instituto Igarapé. Nota Estratégica 30, p. 1-32, 2018. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/09/Uma-estrate%CC%81gia-para-a-governanc%CC%A7a-da-seguranc%CC%A7a-ciberne%CC%81tica-no-Brasil.pdf>. Acesso em: 3 de maio de 2020.

INTELLIGENCE COMMUNITY. **Estratégia Nacional de Inteligência dos Estados Unidos da América**. Estados Unidos, 2019. Disponível em: <https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf>. Acesso em: 13 de março de 2020.

INTERNET WORLD STATS. **World Internet Users and 2019 Population Stats**. Disponível em: < https://www.internetworldstats.com/stats.htm>. Acesso em: 30 de jan. 2020.

INTERNATIONAL TELECOMMUNICATION UNION. **Overview of cybersecurity**. ITU-T X.1205. 64f. 2008.

ISRAEL DEFENSE FORCES. **Estratégia Oficial das Forças de Defesa de Israel (IDF)**. Harvard Kennedy School. Belfer Center for Science and International Affairs English Translation. Israel Defense Forces. Special Report, Cambridge, 2016. Disponível em: < https://www.belfercenter.org/israel-defense-forces-strategy-document>. Acesso em: 28 de março de 2020.

JIANG, Tianjiao. **From Offense Dominance to Deterrence: China's Evolving Strategic Thinkin on Cyberwar**. Chinese Journal of International Review, WSPC & SIRPA of SISU, vol. 1, nº 2, 23f, 2019. DOI: 10.1142/S2630531319500021.

JOINT CHIEFS OF STAFF. **Estratégia Militar Nacional dos Estados Unidos da América**. Departamento de Defesa (DoD), Estados Unidos, 2011. Disponível em: <https://www.globalsecurity.org/military/library/policy/dod/2011-national-military-strategy.pdf>. Acesso em: 8 de abril de 2020.

KAPTO, A. S. **Cyberwarfare: Genesis and Doctrinal Outlines**. Herald of the Russian Academy of Sciences, Vol. 83, nº4, p. 357-364, 2013.

KHANNA, Pallavi. **State Sovereignty and Self-Defence in Cyberspace**. BRICS Law Journal, New Delhi, vol. 5 (4), p. 139-154, 2018.

KIRSCH, Cassandra M. **Science fiction no more: cyberswarfare and United States**. Denver Journal of International Law and Policy. Vol. 40:4, p. 620-647, 2012.

KLIMBURG, Alexander. **Mobilising Cyber Power**. Survival, vol 53 (1), p. 41-60, 2011.

LEINIER, Barry M. et al. **A Brief History of Internet**. ACM SIGCOMM Computer Communication Review, vol. 39, nº 5, 2009. Disponível em: < https://www.internetsociety.org/internet/history-internet/brief-history-internet/>. Acesso em: 5 de fev. 2020.

LEWIS, James A. **Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States**. Inter-American Development Bank (IDB). Observatory Cybersecurity in Latin America and the Caribbean. Discussion Paper nº IDB-DP-457, 2016.

LOBATO, Luisa; KENKEL, Kai M. **Discourses of cyberspace securitization in Brazil and in the United States**. Revista Brasileira de Política Internacional, nº 58 (2), p. 23-43, 2015. http://dx.doi.org/10.1590/0034-7329201500202.

LOPES, Gills V; NETO, Walfredo B. **A Questão da Fronteira Cibernética no Âmbito das Relações Internacionais Cibernéticas (CiberRI).** In: Encontro Nacional da Associação Brasileira de Relações Internacionais (ABRI), 5ª edição, 2015, Belo Horizonte, p. 1-16.

MACHADO, Jussara O. **Ciberguerra: conceitos, doutrinas, estratégias, operações, instituições e o caso dos Estados Unidos**. 2014. 126f. Dissertação de Mestrado. Pontifícia Universidade Católica de Minas Gerais. Belo Horizonte, 2014.

MALAGUTTI, Marcelo. **Ciberespaço: Instrumento Geopolítico com implicações para o Brasil?.** 6º Encontro Nacional da Associação Brasileira de Relações Internacionais (ABRI). Belo Horizonte, p. 1-15, 2017.

MARTINS, Marco. **Ciberespaço: Uma Nova Realidade para a Segurança Internacional**. Revista sobre Cibersegurança do IDN. Lisboa. Nº 133. pp. 32-49. 2012.

MILITÃO, Octávio Pimenta. **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional**. 2014. 89f. Dissertação de Mestrado – Mestrado em Ciência Política e Relações Internacionais da Universidade Nova de Lisboa, Universidade de Lisboa, Lisboa, 2014.

MINISTÉRIO DA DEFESA. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Ministério da Defesa. Brasília, Brasil, 2012a. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 25 de abril de 2020.

MINISTÉRIO DA DEFESA (MD). **Doutrina Militar de Defesa Cibernética**. Portaria Normativa nº 3.010. Brasil, 2014. Disponível em: <https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em 30 de abril de 2020.

MINISTÉRIO DA DEFESA (MD). **Política Cibernética de Defesa**. Portaria Normativa nº 3.389. Brasil, 2012b. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf>. Acesso em: 30 de abril de 2020.

MINISTRY OF FOREIGN AFFAIRS. **Estratégia Internacional de Cooperação no Ciberespaço**. República Popular da China, 2017. Disponível em: < https://www.scio.gov.cn/32618/Document/1543874/1543874.htm>. Acesso em: 23 de março de 2020.

MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY. **Regulamentos sobre a Proteção do Direito de Comunicação na Rede de Informações**. República Popular da China, 2017a. Disponível em: < www.itsec.gov.cn/fgbz/xgfg/201711/t20171130_17941.html>. Acesso em: 25 de março de 2020.

MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY. **Regulamentos sobre o Gerenciamento de Serviços Comerciais de acesso à Internet**. República Popular da China, 2017b. Disponível em: < www.itsec.gov.cn/fgbz/xgfg/201711/t20171130_17940.html>. Acesso em: 26 de março de 2020.

MINISTRY OF PUBLIC SECURITY. **Disposições sobre Supervisão e Inspeção de Segurança na Internet por Órgãos de Segurança Pública**. República Popular da China, 2018. Disponível em: <www.gov.cn/gongbao/content/2018/content_5343745.htm>. Acesso em: 25 de março de 2020.

MIRANDA, Guilhermina L. **Limites e possibilidades das TIC na educação**. Revista de ciências da educação. Lisboa, nº 3, mai/ago 2007. Disponível em: < http://ticsproeja.pbworks.com/f/limites+e+possibilidades.pdf>. Acesso em: 26 de jan. 2020.

MONTEIRO, Luís. **A Internet como meio de comunicação: Possibilidades e Limitações**. In: XXIV Congresso Brasileiro de Comunicação. Campo Grande, MS. 2001. p. 27-37.

MOREIRA, William de Sousa. **Ciência e Tecnologia Militar: “política por outros meios”?**. Revista da Escola de Guerra Naval, Rio de Janeiro, v.18, n.2, jul./dez. 2012. Disponível em: < https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/314/239>. Acesso em: 25 jan. 2020.

NATIONAL INTERNET INFORMATION OFFICE. **Medidas de Gerenciamento de Segurança de Dados**. República Popular da China, 2019. Disponível em: < www.moj.gov.cn/news/content/2019-05/28/zlk_235861.html>. Acesso em: 25 de março de 2020.

NATO CCD COE. **Tallinn Manual on The International Law Applicable to Cyber Warfare**. New York. Cambridge University Press. 215f. 2013.

NYE, Joseph. **Cyber Power**. Harvard Kennedy School: Belfer Center for Science and International Affairs, Cambridge, p. 1-24, 2010.

NYE, Joseph. **Deterrence and Dissuasion in Cyberspace**. International Security, Vol. 41, nº 3, p. 44-71, 2017.

OCDE. **Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy**. OCDE, 2012. Disponível em: <http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>. Acesso em: 28 de jan. 2020.

OFFICE OF THE CENTRAL CYBERSPACE AFFAIRS COMMISION. **Lei de Segurança Cibernética da República Popular da China**. República Popular da China, Beijing, 2016. Disponível em: <www.cac.gov.cn/2016-11/07/c_1119867116.htm>. Aceso em: 21 de março de 2020.

PAULSEN, Celia et al. **NICE: Creating a Cybersecurity Workforce and Aware Public**. US National Institute of Standards and Technology. IEEE Security & Privacy, vol. 10, p. 76-79, 2012. DOI: 10.1109/MSP.2012.73.

PERNIK, Perit et al. **National Cyber Security Organisation: United States**. CCDCOE NATO Cooperative Cyber Defence Centre of Excellence. Tallin, Estonia, 2016. Disponível em: <https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf>. Acesso em: 15 de março de 2020.

POLATIN-REUBEN, Dana; WRIGHT, **Joss. An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet**. University of Oxford, UK, p. 1-10, 2014. Disponível em: < https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>. Acesso em: 20 de maio de 2020.

PORTELA, Lucas S. **Movimentos Centrais e Subjacentes no Espaço Cibernético do Século XXI**. 2015. 150f. Dissertação de Mestrado. Escola de Comando e Estado-Maior do Exército: Escola Marechal Castello Branco. Rio de Janeiro, 2015.

PRIME MINISTER’S OFFICE. **Resolução 3611**. Estado de Israel, 2011. Disponível em: < https://www.gov.il/he/Departments/policies/2011_des3611>. Acesso: 27 de março de 2020.

PRIME MINISTER’S OFFICE. **Estratégia Nacional de Segurança Cibernética de Israel em Resumo.** National Cyber Directorate. Estado de Israel, 2017. Disponível em: < http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf>. Acesso em: 28 de março de 2020.

PRIME MINISTER’S OFFICE. **Políticas de Regulamento de Profissões de Segurança Cibernética no Estado de Israel**. National Cyber Bureau. Estado de Israel, 2015.

Disponível em: < http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf>. Acesso em: 1 de abril de 2020.

QI, Aimin et al. **Assessing China's Cybersecurity Law**. Computer Law & Security Review, vol. 34, p. 1342-1354, Reino Unido, 2018.

RAZA, Salvador. **The security and defense matrix: Concepts matter in defense analysis?.** Defense and Security Analysis, vol. 21, nº 1, p. 67-78, 2005.

RYAN, Johnny. **A history of the Internet and the Digital Future**. Reaktion Books, London, 2010.

RUDZIT, Gunther; NOGAMI, Otto. **Segurança e Defesa Nacionais: conceitos básicos para uma análise**. Revista Brasileira de Política Internacional. vol. 53 (1). p. 5-24, 2010.

SALTZMAN, Ilai. (2013). **Cyber posturing and the offense-defense balance**. Contemporary Security Policy, 34(1), p. 40–63. 2013.

SCHMITT, Michael. **France's Major Statement on Internacional Law and Cyber: An Assessment: Use of Force, Sovereignty and More.** Just Security, 2019. Disponível em: < https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/>. Acesso em: 11 de maio de 2021.

SEABRA, Miguel P. **O Conceito de Fronteira: Uma abordagem multifacetada**. Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto. Instituto de Estudos Superiores Militares. Portugal, Lisboa, 68f, 2012.

SHEN, Hong. **China and global internet governance: toward an alternative analytical framework**. Chinese Journal of Communication. Vol. 9. Nº. 3, p. 304-324, 2016. https://doi.org/10.1080/17544750.2016.1206028.

SINGER, P.W; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What Everyone Needs to Know**. 1. ed. Oxford: Oxford University Press, 2013.

SOUZA J. Alcyon F; STREIT, Rosalvo E. **Segurança cibernética: política brasileira e a experiência internacional**. Revista do Serviço Público, nº 68 (1), p. 107-130, Brasília, 2017.

SPERL, Frank; THIA, Yong Wah. **Role of the U.S Government in the Cybersecurity of Private Entities**. Naval Postgraduate School. California. MBA Professional Report. Institutional Archive of the Naval Postgraduate School. 2017. Disponível em: < https://calhoun.nps.edu/bitstream/handle/10945/56812/17Dec_Sperl_Thia.pdf?sequence=1&isAllowed=y>. Acesso em: 10 de abril de 2020.

STATE COUNCIL INFORMATION OFFICE. **Defesa Nacional da China na Nova Era**. República Popular da China, Beijing, 2019. Disponível em: < http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm>. Acesso em: 2 de abril de 2020.

TABANSKY, Lior and BEM-ISRAEL, Isaac. **Cybersecurity in Israel**. SpringerBriefs in Cybersecurity, New York, 2015. DOI 10.1007/978-3-319-18986-4.

THE GOVERNMENT SECRETARY. **Resolução 2443**. Estado de Israel, Jerusalem, 2015a. Disponível em: <https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2443-Advancing-National-Regulation-and-Governmental-Leadership-in-Cyber-Security.pdf>. Acesso em: 27 de março de 2020.

THE GOVERNMENT SECRETARY. **Resolução 2444**. Estado de Israel, 2015b. Disponível em: <https://www.gov.il/he/departments/policies/2015_des2444>. Acesso em: 28 de março de 2020.

UNITED NATIONS. **Human Development Report**. United Nations Development Programme. Oxford University Press. New York, 1994. Disponível em: < http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf>. Acesso em: 14 de janeiro de 2021.

U.S ARMY WAR COLLEGE. **Information Operations Primer: Fundamentals of Information Operations**. Department of Military Strategy. Estados Unidos, 2011. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a555809.pdf>. Acesso em: 17 de março de 2020.

VALO, Janne. **Cyber Attacks and the Use of Force in International Law**. 2014. 101f. Dissertação de Mestrado. University of Helsinki, 2014.

WEBER, Max. **Ensaios de Sociologia**. In: GERTH, H.H; MILLS, C.Wright (Ed), *MAX WEBER*. Livros Técnicos e Científicos S.A, Rio de Janeiro, 5ª ed, 1982. Disponível em:<https://edisciplinas.usp.br/pluginfile.php/3952424/mod_resource/content/1/Max%20Weber%20-%20Ensaios%20de%20Sociologia%20-%20Gerth%20%20Mills.pdf>. Acesso em: 15 de março de 2020.

WENDT, Alexander. **Social Theory of International Politics**. 1. ed. Cambridge: Cambridge University Press, 1999.

WHITE HOUSE. **Revisão da Política para o Ciberespaço**. Estados Unidos, 2009. Disponível em: <https://fas.org/irp/eprint/cyber-review.pdf>. Acesso em: 13 de março de 2020.

WHITE HOUSE. **Estratégia Nacional para Proteger o Ciberespaço**. Estados Unidos, 2003. Disponível em: <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>. Acesso em: 16 de março de 2020.

WHITE HOUSE. **Estratégia de Segurança Nacional dos Estados Unidos da América**. Estados Unidos, 2017. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>. Acesso em: 10 de fevereiro de 2020.

WHITE HOUSE. **Estratégia Cibernética Nacional dos Estados Unidos da América**. Estados Unidos, 2018. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Acesso em: 10 de fevereiro de 2020.

WORLD ECONOMIC FORUM. **The Global Risks Report**. 14. Ed. Geneva, 2019.

ZENG, Jinghan et al. **China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"**. Politics & Policy. Policy Studies Organization, vol. 45, nº 3, p. 432-464, 2017.